Al-Khwarizmi Engineering Journal, Vol. 19, No. 3, September, (2023)
P. P. 44- 55

Al-Khwarizmi Engineering Journal

High Transaction Rates Performance Evaluation for Secure E-government Based on Private Blockchain Scheme

Osama Ibraheem Kadhm* **Ali hussein Hamad****

*,**Department of Information and Communications/Al-Khwarizmi College of Engineering/ University of Baghdad/Baghdad/Iraq

Corresponding author *Email: ooosaamaa84@gmail.com

**Email: ahamad@kecbu.uobaghdad.edu.iq

(Received 14 March 2023; Accepted 18 June 2023)

https://doi.org/10.22153/kej.2023.06.002

Abstract

The implementation of technology in the provision of public services and communication to citizens, which is commonly referred to as e-government, has brought multitude of benefits, including enhanced efficiency, accessibility, and transparency. Nevertheless, this approach also presents particular security concerns, such as cyber threats, data breaches, and access control. One technology that can aid in mitigating the effects of security vulnerabilities within e-government is permissioned blockchain. This work examines the performance of the hyperledger fabric private blockchain under high transaction loads by analyzing two scenarios that involve six organizations as case studies. Several parameters, such as transaction send rate, blockchain size, batch timeout, organization number, and the number of clients, were modified in the two scenarios. The gradual addition of organizations was also observed to determine the impact of multi-organization on the throughput, latency, and scalability of the system. By increasing the block size to approximately 100 transactions per block, acceptable performance and latency results are attained. The throughput and latency findings are accepted for three or four organizations, but when many organizations are added, throughput and latency begin to suffer from poor performance. Also, many tests show that increased block timeout for high sending rates positively affects the throughput and latency.

Keywords: *e-government, private blockchain, fabric, hyperledger caliper, performance analysis.*

1. Introduction

Information and communications technology (ICT) developments have totally changed how governments interact with the people they govern and offer services. E-government has made it possible for citizens to conveniently access government services and information online, anytime, from anywhere, and without having to physically visit government offices [1,2]. This change has resulted in increased transparency, accountability, and citizen involvement while also considerably improving accessibility, convenience, and efficiency in government services. E-government has also resulted in lower administrative expenses, higher productivity, and an overall improvement in the quality of public services. The expansion of e-government is anticipated to continue and bring about additional changes in how governments function and engage with their citizens as digital tools and platforms become more widely accessible [3].

The main goals of E-governments are to streamline and enhance the processes of the governments in order to increase accessibility and effectiveness for both citizens and business while using government services and carrying out transactions. By increasing public awareness of government activities, E-government has an opportunity to strengthen openness and

accountability [4]. This can be done by improving access to public records, publishing government data and information online, and allowing individuals to follow the development of government projects and activities. Additionally, e-government initiatives can stimulate economic growth by supporting corporate growth and enticing investment. One noteworthy instance is the simplification of procedures for registering and approving businesses, which can help create a climate more conducive to business expansion [5]. Despite the many services the electronic government provides, but some people are afraid to use it because of security problems that e-government faces, including Identity theft of sensitive personal data by hackers. Also, E-government systems are vulnerable to cyber-attacks which can steal the information stored in secured systems by compromising them. Cyber-attacks can come in many forms, including phishing, ransomware, and denial-of-service attacks. Technical problems with e-government systems can also make people hesitant to use them [6].

The security of e-governments can be strengthened by many technologies. These include cloud computing, biometric authentication, multi-factor authentication (MFA), public key infrastructure (PKI), and blockchain technology [7].

Blockchain technology is a system of distributed digital ledgers for transactions that are computer-based. If the block is a part of the chain, it cannot be changed or deleted. A history of transactions is kept in each block of the chain. As a result, all transactions on the blockchain are transparent and permanent [8,9]. The technology behind the blockchain is based on cryptography and decentralized consensus. Each node in the network has a copy of the blockchain, and each node must validate and agree on each transaction before it is added to the chain. This consensus mechanism ensures that the blockchain is secure, transparent, and tamper-proof [10,11]. The Bitcoin blockchain, a decentralized database for Bitcoin transactions, is the most well-known application of blockchain technology. Yet, blockchain technology has a wide range of uses outside of cryptocurrencies, such as supply chain management, electoral processes, and digital identity confirmation. With blockchain technology, e-government security could be increased in several ways, including the ability of blockchain to produce an unchangeable transaction history; that is, a transaction that has been added to the blockchain cannot be altered or deleted once it has been added [12,13].

This paper aims at contributing in the development of a secure and efficient E-government system using hyperledger fabric blockchain technology with high transaction rates reaching 200 tps. Also, it discusses the scalability and performance of the system by engaging six organizations with up to 150 clients.

This paper assesses the performance of fabric blockchain by evaluating transaction latency, parallel throughput, and scalability under varying blockchain sizes, batch timeouts, clients, and organizations with a transaction rate of 200 tps. The work includes six fabric firms and benchmarks fabric performance with the caliper.

The rest of this paper is structured as follows: Section 2 presents the related work. Section 3 explains hyperledger fabric permissioned blockchain, and Section 4 details a multi-organization system with several experiments. Also, the performance evaluation and analysis of private blockchains are described in this section. Finally, Section 5 presents the conclusions.

2. Related Work

Because of the essential role of the blockchain technology in developing new algorithms, a growing number of researchers have recently shifted their focus to its evaluation and analysis.

An empirical study comparing the capabilities of hyperledger fabric and Ethereum, two of the most notable blockchain platforms has been carried out by M. Dabbagh and colleagues [14]. Their performance was measured using four criteria: success rate, average latency, throughput, and resource usage. The results of performing one hundred transactions demonstrated that when compared with Ethereum across all four performance measures, hyperledger fabric is superior overall.

C. Wang and X. Chu [15]. investigated the performance characteristics of the hyperledger fabric at each step, including the execute, order, and validate phases. In addition to that, they investigated the ordering services, such as Solo, Kafka, and Raft. The findings of their experiments revealed that the execution phase exhibited a robust scalability when the OR endorsement policy was used, but this was not the case when the AND endorsement strategy was used. They also discovered that the validation phase was likely to be the system bottleneck because of the

slow validation speed of the chaincode. This was another finding that they made.

An investigation into the functionality and scalability of major private blockchain platforms, such as Ethereum, Quorum, Corda, and Hyperledger Fabric, was carried out by A. A. Monrat et al [16]. In order to evaluate each of these platforms, they first changed the workloads and then determine the performance evaluation metrics using throughput and network latency. The caliper tool was used in the test that Saeed et al. [17] conducted to examine the effect of the electronic voting workload on the hyperledger fabric framework. This test looked at a variety of factors, including latency and performance. A great variety of alternative scenarios could be simulated and tested by making simultaneous changes to the transaction transmission speeds, block sizes, timeouts of the block, and organizations. Caliper was utilized by W. Choi and J. W. -K. Hong [18] in order to conduct an analysis of an Ethereum private network in addition to the Ropsten testnet. According to their tests and comparisons, the Ethereum private network performs superior to that of the Ropsten testnet. In addition, the findings demonstrated that the results of the transactions could vary depending on the content of the transaction.

Using a Hyperledger Fabric GoLevelDB (HLF-GLDB) benchmark allowed T. Nakaike et al [19] to assess the performance of database systems that are employed in hyperledger fabric for discovering areas of optimization. As a stand-alone benchmark is used for simulating database accesses in hyperledger fabric, they developed HLF-GLDB. The findings of their studies indicated that the data compression feature of GoLevelDB is a significant performance barrier in hyperledger fabric. Turning off the data compression feature resulted in 54% improvement in the system's overall performance. They also discovered that the size of a database substantially impacts its performance; specifically, they observed that the performance decreased by 25% when the size of the database was raised by a factor of four.

In summary, references [14] and [17] were the closest to our work. In reference [14], there are many differences between their work and ours. Firstly, their work was limited to a maximum of 100 tps and only involved three organizations. In contrast, our work focused on higher transaction rates of up to 200 tps and included up to six organizations. Secondly, while they relied solely on the block size of the blockchain, we also considered the block timeout, which is crucial for platform performance and scalability. Lastly, their approach used the ORing raft algorithm, which only required the agreement of one organization to confirm a transaction. In contrast, we utilized a more secure ANDing algorithm that requires the agreement of all organizations before a transaction can be confirmed.

Reference [17], Their research focused on the e-voting process. Additionally, they included up to three different organizations with fewer clients (under 20). What makes our work unique is that, in order to show the scalability and performance of our system, we tried to involve more organizations (up to six) and clients (up to 150).

3. Hyperledger Fabric platform

Hyperledger fabric is an open-source permissioned blockchain framework that aims at creating enterprise-grade distributed ledger technology for business applications. It allows developers to create smart contracts and applications using a modular architecture.

Hyperledger fabric is a unique blockchain platform designed for use cases where privacy, scalability, customization, and performance are critical. The fabric allows organizations to control who has access to their data and provides a range of privacy-enhancing features such as private channels, private data collections, and identity management [20,21]. Hyperledger fabric is highly scalable in addition it can support many transactions per second. It achieves this through its unique approach to consensus, which allows for parallel transaction processing and off-chain data storage [22].

The Membership Service Provider (MSP), Fabric Certificate Authority (CA), Peer nodes, ordering service, Chaincode, Ledger, Consensus protocol, and Fabric Software Development Kit (SDK) are among the major components of Hyperledger Fabric [23,24]. The MSP is essential for handling and confirming network users' digital identities, including clients, peers, and orderers, in the Hyperledger Fabric ecosystem. Its main job is to make sure that none except trusted and authorized parties can access the shared ledger or connect with other network members.

For users of networks, the Certificate Authority (CA) acts as a reliable provider of digital identities, facilitating safe exchange of

information and transactions. Its primary duty is to create and maintain digital certificates that verify network users' identities and protect transaction secrecy, integrity, and non-repudiation. Contrarily, the Ordering Service is vital to reaching an agreement and preserving the sequence of transactions among all nodes.

Transactions are received from clients and disseminated to all nodes by the system. Then, using a consensus mechanism, it groups these transactions into blocks and puts them in a particular order. The ordering service offers the blocks to all network peers for validation and execution once they have been appropriately ordered.

The chaincode works as a set of rules directing the network's operation. Its goal is to simplify a range of network functions, including the execution of smart contracts, allowing for the execution of transactions and the accompanying record changes. The ledger, on the other hand, is comparable to a large record book that carefully documents and keeps a complete log of all transactions taking place within the network. It's shared by everyone in the network and can't be changed once something is written down. The Fabric SDK is a toolkit that enable developers to interact with the network, submit transactions, and look at the ledger. Consensus protocols ensure that everyone in the network agrees on what transactions happened and in any order. This helps to ensure that everything is fair and transparent. All of this makes the network secure, transparent, and auditable. Figure 1 shows the basic flow diagram of the fabric platform.

4. Proposed Multi-organization System

Six interconnected organizations will conduct performance tests on the hyperledger fabric platform using the latest release of the software with long-term support, v2.4 (LTS). The primary objective is to determine how various configuration settings, such as the block size, block timeout, number of clients, and number of organizations influence the throughput, latency, and scalability of the platform.

As showed in figure 2, each organization has one fabric SDK through it, the clients can communicate with other entities in the fabric platform. One CA which is responsible for granting certificates to members, one MSP tasked with keeping track of authorized entities. Each organization also has one committer which commits the transaction to the ledger, and one anchor peer which is responsible for communications with the other organizations. Besides, all the organizations are connected to one orderer node which depends on a raft algorithm and is responsible for maintaining the order and consistency of transactions on the blockchain.

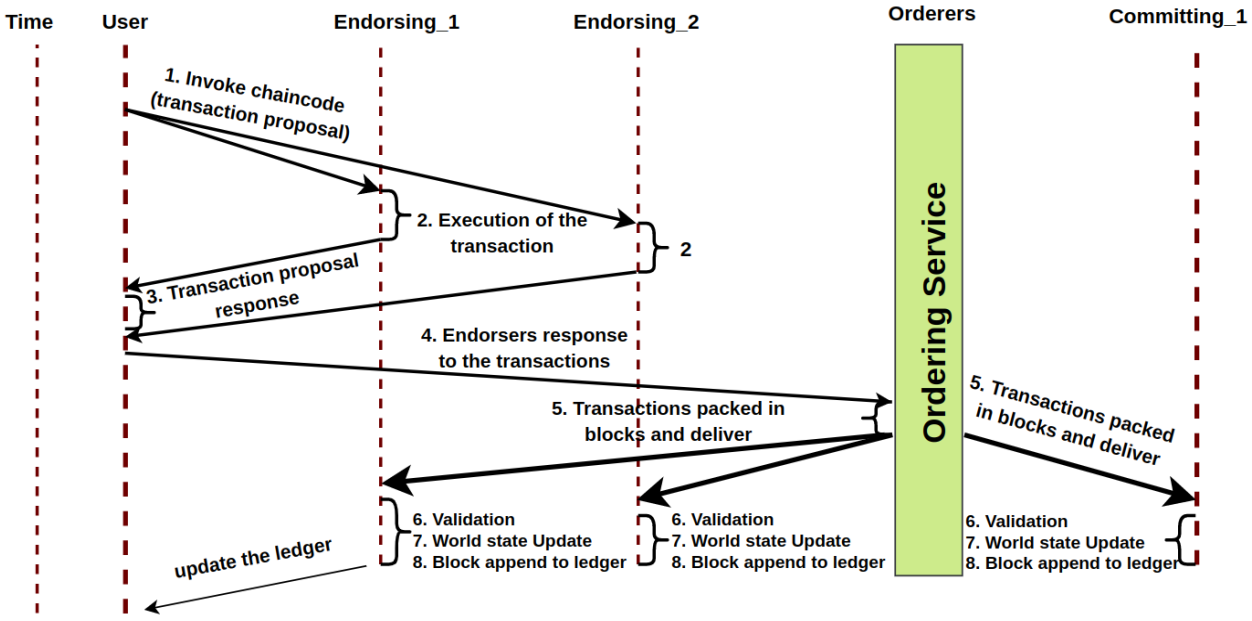


Fig. 1. Basic flow diagram of hyperledger fabric [6].

Hyperledger caliper is a tool that can evaluate and verify the performance of various hyperledger platforms, including the fabric by measuring metrics such as latency, throughput, and scalability.

In this work, we have configured the following options: a transaction rate of 200 tps, serving clients ranging from 1 to 150, and block timeouts set at 1 second, 2 seconds, and 5 seconds.

The design shown in Figure 2 distinguishes itself from other designs in multiple ways. Firstly, it incorporates six distinct organizations, whereas conventional designs usually involve up to three organizations. Using six organizations provides more robust proof of scalability for the platform compared to three organizations. Secondly, this design can accommodate up to 150 clients or even more, a significant increase compared to other designs that typically cater to fewer than 150 clients. Thridly, we have relied on two factors - the block timeout and the block size - to improve the performance and scalability of the system. In contrast, other implementations only rely on the block size. Finally, we are able to achieve transmission rates of 200 tps, while other designs only reached 100 tps.

To test the system's throughput, latency, and scalability, we have employed the following two scenarios in this work:

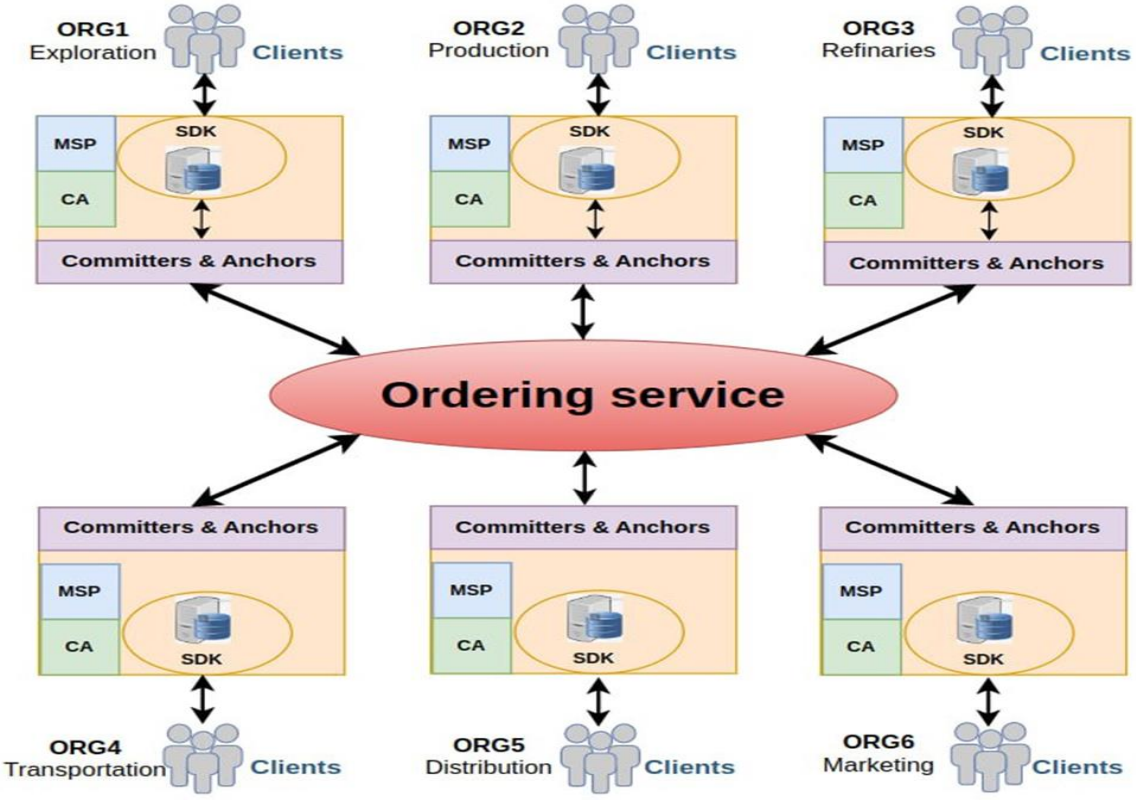


Fig. 2. multi-organization scheme.

4.1 Scenario one: varying the block size of the blockchain.

Three rounds of testing have been done in this scenario to gauge the system's throughput and typical latency. A total of 10,000 transactions are included in each round. The maximum sending rate we achieved in this test with the caliper is set to 200 transactions per second in all rounds, with the block size increasing from (50, 100, and 150) transactions per block and the number of clients increasing from 50 to 100 and 150 in each round. The batch timeout's default setting was 2 seconds. As shown in Figure 3(a), when the sending rate is set to be 200 tps and the block size to 50 (Tx/block), the throughput was acceptable on the first three organizations, especially with a small number of users in the system, which was about 70 tps for 50 clients, about 57 tps for 100 clients, and about 30 tps for 150 clients. But with increasing number of organizations to six and

number of clients to 150, the throughput dropped sharply until it reached only 6 or 7 tps.

The case is the same for latency, as shown in Figure 3(b). That is, for the first three organizations and few clients, the latency was good which reached about 6 seconds, but when the number of organizations increases to six and the number of clients increases to 150, the latency becomes very high (about 45 seconds).

Figure 3(c) and 3(d) shows that the increase of the block size to 100 (Tx/block) had better impact on the throughput and latency. The throughput increased to about 75 tps at three organizations and 50 clients, about 63 tps for 100 clients, and about 40 tps at 150 clients.

But from experiments, we found that when the block size increased to 150 (Tx/block). This increase negatively impacted the throughput and latency, as shown in Figures 3(e) and 3(f); the throughput declined to about 54 tps at 50 clients and 3 organizations, about 50 tps at 100 clients, and about 30 tps at 150 clients.

The experiments also show that under full load includes engaging all six organizations and 150 clients; the throughput and latency results of block size = 50 were about 7 tps and 47 seconds as shown in figures 3(a) and 3(b). While the throughput increaed to about 10 tps and the latency decreased to about 45 seconds at block size = 100, as in figures 3(c) and 3(d). also, at block size = 150 (Tx/block) the throughput decreased to about 6 tps and the latency increased to about 50 seconds as in figures 3(e) and 3(f).

The experiments described above show that the optimal combination of throughput and latency was achieved using 100 transactions per block size. Therefore we will depend on 100 (Tx/block) in the next scenario.

4.2 Scenario two: varying the blocking timeout of the blockchain.

Three rounds of testing have been done in this situation as well to gauge the throughput and latency of the system. Ten thousand transactions are included in each round. Because this block size produced the most significant results in scenario one, we have fixed the block size to 100 transactions per block for all rounds. The blocking timeout is then increased from (1, 2, and 5) seconds for three experiments.

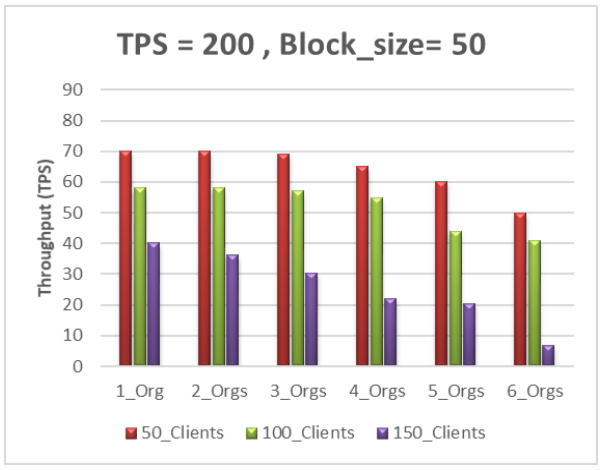
After that, we increased the number of clients in each round from 50 to 100 and 150 in all six organizations. Next, we set the sending rate to 200 tps, which is the maximum rate we have reached in this experiment with the caliper.

Figures 4(a,c) demonstrate that the throughput was enhanced when we increased the blocking timeout from 1 second to 2 seconds; that is, under heavy load, which includes engaging all six organizations and 150 clients, the throughput was about 5 tps at 1 second timeout and about 11 tps at 2 seconds. While the throughput reached its maximum level (about 20 tps) when the blocking timeout is increased to 5 seconds, as in Figure 4(e).

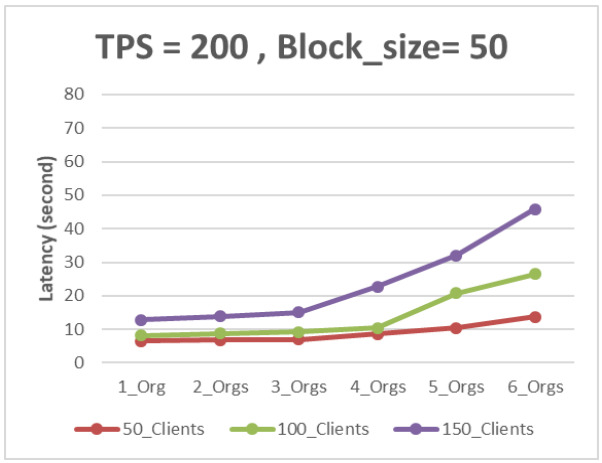
Regarding the latency (also under heavy load, which includes engaging all six organizations and 150 clients), Figures 4(b,d) show that the latency decreased whenever the blocking timeout was increased from 1 second to 2 which was about 56 seconds at timeout = 1 second and about 45 seconds at 2 seconds timeout. Also figure 4(f) shows that the latency decreased to its lowest level (about 39 seconds) when we increased the blocking timeout to 5 seconds.

The block timeout reduction suggests that the block was cut before it had reached its maximum capacity. The findings showed that increasing block timeout better impacts system performance, particularly with big block sizes.

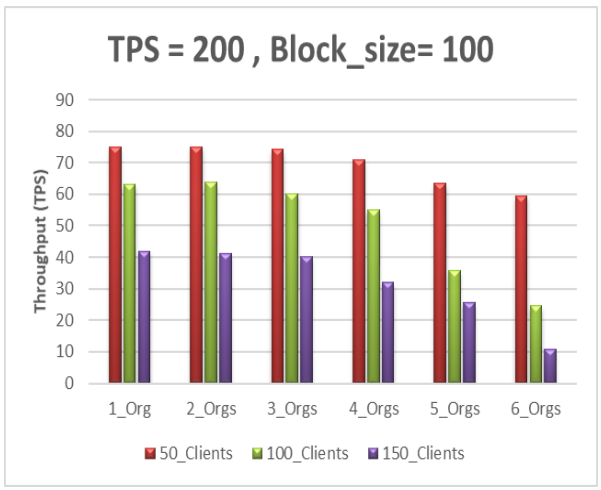
While increasing the batch timeout may seems like a straightforward way to address a slow network or high latency issues, it can come with some disadvantages. A higher latency improves the likelihood of including more transactions in a single block. The size of a block expands in proportion to the number of transactions in it. Larger block sizes can lead to more extended propagation and validation times, increasing the likelihood of network congestion and reducing the overall network throughput. Also, the consensus mechanism in hyperledger fabric requires that all nodes in the network agreemet on the order of transactions.



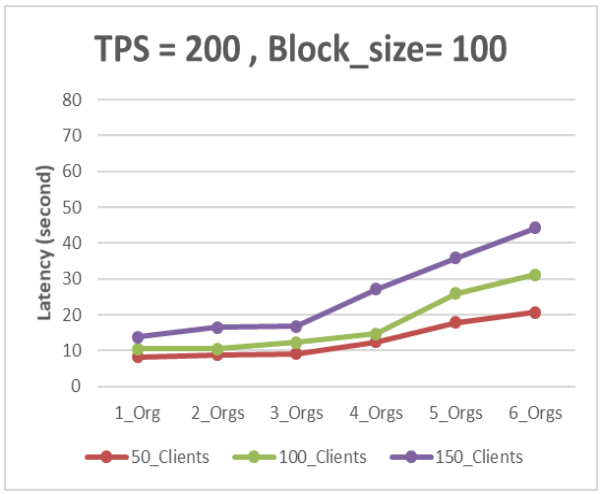
3.a



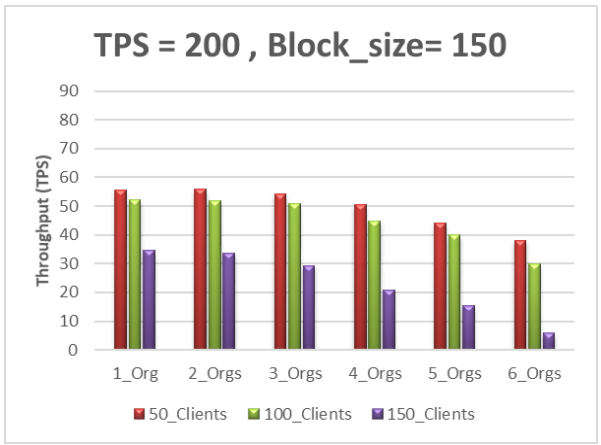
3.b



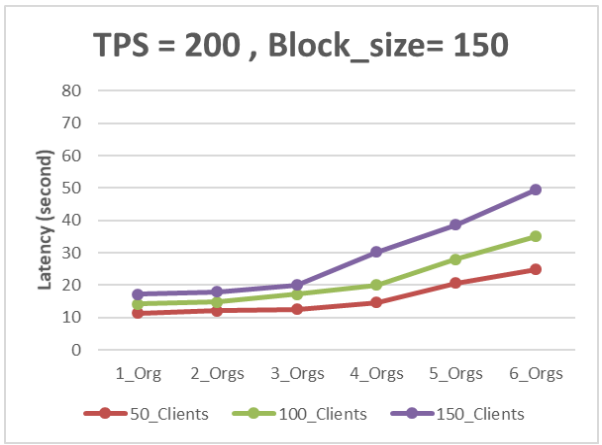
3.c



3.d



3.e

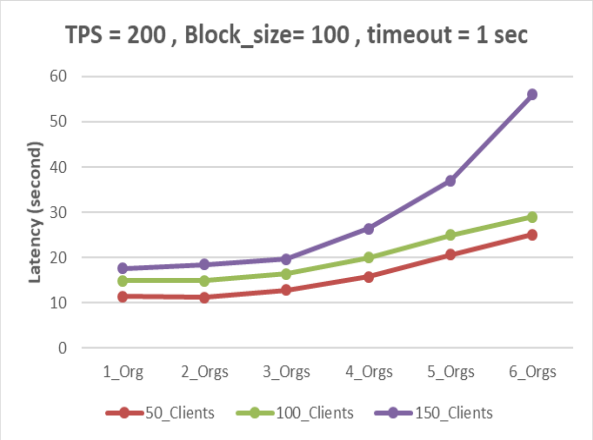


3.f

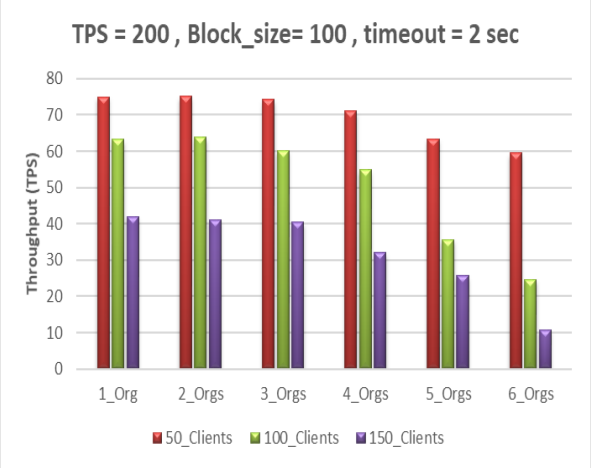
Fig. 3. (a,b,c,d,e,f). Throughput and latency results of increasing the block size.

Some nodes could become out of synchronization with the rest of the network if the batch timeout is configured too high. Lower consensus efficiency could come from this, affecting the network as a whole.

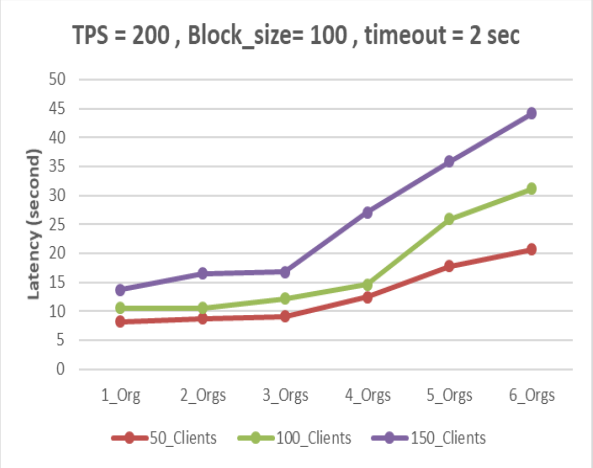
4.a



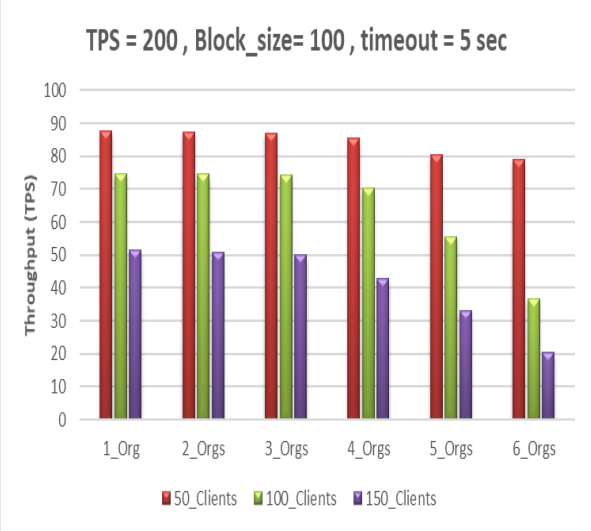
4.b



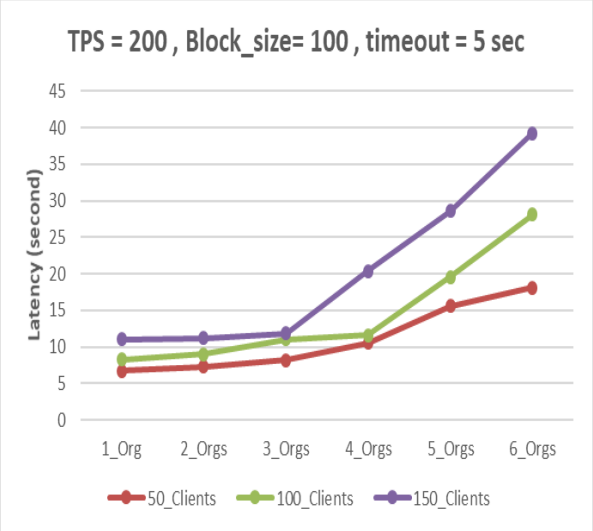
4.c



4.d



4.e



4.f

Fig. 4. (a,b,c,d,e,f). Throughput and latency results of increasing the block timeout.

5. Conclusions

In this research, we investigate how a workload generated by a multi-organizational system affects the functionality of a blockchain running on the hyperledger fabric platform. We have concentrated on evaluating the average latency, scalability, and throughput parameters. We did various tests to undertake our analysis, varying parameters including transmission rates, block sizes, block timeouts, client count, and overall organization count. In the end, we found that the complexity of the smart contracts, the hardware configuration, and the design of the blockchain network all contribute to its success. Our findings have revealed the following results in greater details:

1- We found an intriguing correlation between block timeout, block size, and the performance os the system. We specifically saw improvements in the throughput, latency, and scalability of the platform when we raised the block size from 50 to 100 transactions per block while keeping a block timeout of 2 seconds. However, we have noticed a decrease in the throughput of the platform and an increase in latency when we steadily increased the block size to 150 transactions per block. It also implies that increasing the number of transactions in a block beyond 100 is unlikely to have a favorable effect on the platform's performance.

2- In most cases, we have discovered that, whether there are a small number of clients and organizations or large number of clients and organizations, the ideal balance between throughput and latency was typically obtained with a block size of 100 transactions per block. Both speed and latency consistently performed best with this block size.

3- Our tests have revealed that increasing the block timeout from 1 second to 2 seconds and up to 5 seconds result in a significant improvement in the throughput and average latency, under both moderate and full load conditions. However, increasing the block timeout from 2 seconds to 5 seconds can also have some drawbacks, especially for latency-sensitive applications because longer validation and commit times for transactions can increase the overall transaction latency. Additionally, setting the block timeout too high can increase the network resource utilization, as nodes must maintain transaction state for longer periods. Finally, the extension of block timeout could potentially compromise the security of the platform. This is because longer timeouts provide more opportunities for intruders to attempt to capture the data. Therefore, a careful planning and control are required when increasing the block timeout.

Acknowledgments

This work is supported by the information and communications engineering department Al-Khawarizmi Engineering College, University of Baghdad.

References

[1] A. M. K. . AL-Ghraibawy, “The Influence of Organizational Power on the Achievement of Entrepreneurship for Business Organizations An Analytical Study of the Views of a Sample of Managers in the Iraqi Ministry of Education”, JEAS, vol. 28, no. 131, pp. 59–82, Mar. 2022. DOI: https://doi.org/10.33095/jeas.v28i131.2234

[2] Marian STOICA and Bogdan GHILIC-MICU (2020)," E-Government in Romania – a Case Study", Journal of e-Government Studies and Best Practices, Vol. 2020 (2020), Article ID 608643, http://dx.doi.org/10.5171/2020.608643

[3] A. S. Elameer, "COVID-19 and real e-government and e-learning Adoption in Iraq," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 323-329, http://dx.doi.org/10.1109/IICETA51758.2021.9717570

[4] Salman, R. H. ., Shiltagh, N. A. ., & Abdullah, M. Z. . (2021). Development of a Job Applicants E-government System Based on Web Mining Classification Methods. *Iraqi Journal of Science*, *62*(8), 2748–2758. https://doi.org/10.24996/ijs.2021.62.8.28

[5] I. M. Hayder, H. A. Younis, I. A. Abed and H. A. Younis, "Services System between Citizens and the E-Government in the Iraqi Ministry of Migration and Displaced," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), Najaf, Iraq, 2020, pp. 117-121, http://dx.doi.org/10.1109/IICETA50496.2020.9318959

[6] Mohsin, M.A., Hamad, A.H. (2022). Performance evaluation of SDN DDoS attack detection and mitigation based random forest and K-nearest neighbors machine learning algorithms. Revue d'Intelligence Artificielle, Vol. 36, No. 2, pp. 233-240. https://doi.org/10.18280/ria.360207

[7] María Isabel Ortiz-Lizcano, Enrique Arias-Antunez, Ángel Hernández Bravo, María Blanca Caminero, Tomás Rojo Guillen, Syong Hyun Nam Cha, Increasing the security and traceability of biological samples in biobanks by blockchain technology, Computer Methods and Programs in Biomedicine, Volume 231, 2023, 107379, ISSN 0169-2607, https://doi.org/10.1016/j.cmpb.2023.107379

[8] Salman, S.A.B., Al-Janabi, S. and Sagheer, A.M., 2022. A Review on E-Voting Based on Blockchain Models. Iraqi Journal of Science, pp.1362-1375. DOI: https://doi.org/10.24996/ijs.2022.63.3.38

[9] U. Bodkhe et al., "Blockchain for Industry 4.0: A Comprehensive Review," in IEEE Access, vol. 8, pp. 79764-79800, 2020, http://dx.doi.org/10.1109/ACCESS.2020.2988579

[10] A. B. Abdulhussein, A. K. Hadi and M. Ilyas, "Design a Tracing System for a Seed Supply Chain Based on Blockchain," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), Najaf, Iraq, 2020, pp. 209-214, http://dx.doi.org/10.1109/IICETA50496.2020.9318792

[11] Ravi Prakash, V.S. Anoop, S. Asharaf, Blockchain technology for cybersecurity: A text mining literature analysis, International Journal of Information Management Data Insights, Volume 2, Issue 2, 2022, 100112, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2022.100112

[12] S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in IEEE Access, vol. 9, pp. 13938-13959, 2021, http://dx.doi.org/10.1109/ACCESS.2021.3051602

[13] A. A. . Hassan, " Blockchain Technology and its Potential Effect on the Banking Industry (China Case Study)", JEAS, vol. 28, no. 131, pp. 133–149, Mar. 2022. DOI: https://doi.org/10.33095/jeas.v28i131.2240

[14] M. Dabbagh, M. Kakavand, M. Tahir and A. Amphawan, "Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum," 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), Kota Kinabalu, Malaysia, 2020, pp. 1-6, http://dx.doi.org/10.1109/IICAIET49801.2020.9257811

[15] C. Wang and X. Chu, "Performance Characterization and Bottleneck Analysis of Hyperledger Fabric," 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore, 2020, pp. 1281-1286, http://dx.doi.org/10.1109/ICDCS47774.2020.00165

[16] A. A. Monrat, O. Schelén and K. Andersson, "Performance Evaluation of Permissioned Blockchain Platforms," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 2020, pp. 1-8, http://dx.doi.org/10.1109/CSDE50874.2020.9411380

[17] 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, Vol. 36, No. 4, pp. 581-587. https://doi.org/10.18280/ria.360410

[18] W. Choi and J. W. -K. Hong, "Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper," 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Tainan, Taiwan, 2021, pp. 325-329, http://dx.doi.org/10.23919/APNOMS52696.2021.9562684

[19] T. Nakaike, Q. Zhang, Y. Ueda, T. Inagaki and M. Ohara, "Hyperledger Fabric Performance Characterization and Optimization Using GoLevelDB Benchmark," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-9, http://dx.doi.org/10.1109/ICBC48266.2020.9169454

[20] Ghassan Al-Sumaidaee, Rami Alkhudary, Zeljko Zilic, Andraws Swidan, Performance analysis of a rivate blockchain network built on Hyperledger Fabric for healthcare, Information Processing & Management, Volume 60, Issue 2, 2023, 103160, ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2022.103160

[21] Radu Godina, Aurélien Bruel, Angela Neves, João C.O. Matias, The Potential of Blockchain Applications in Urban Industrial Symbiosis, IFAC-PapersOnLine, Volume 55, Issue 10, 2022, Pages 3310-3315, ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2022.10.122

[22] J. Ma, Y. Jo and C. Park, "PeerBFT: Making Hyperledger Fabric's Ordering Service Withstand Byzantine Faults," in IEEE Access, vol. 8, pp. 217255-217267, 2020, http://dx.doi.org/10.1109/ACCESS.2020.3040443

[23] The Linux Foundation Project. Available online: https://www.hyperledger.org, Last access in april 2023

[24] The official documentation of hyperledger fabric v2.4 available online, https://hyperledger-fabric.readthedocs.io/. Last access in april 2023.

تقييم وتحليل اداء نظام حكومة الكترونية مؤمنة بطريقة البلوكشين الخاص

اسامة ابراهيم كاظم* علي حسين حمد**

قسم هندسة المعلومات والاتصالات/ كلية الهندسة الخوارزمي/ جامعة بغداد *،**

*البريد الالكتروني: ooosaamaa84@gmail.com

**البريد الالكتروني: ahamad@kecbu.uobaghdad.edu.iq

الخلاصة

ان استخدام التكنولوجيا لتقديم الخدمات العامة والتفاعل مع المواطنين، والمعروفة أيضًا باسم الحكومة الإلكترونية، أفضت إلى العديد من المزايا، مثل تحسين الكفاءة والوصول والشفافية. ومع ذلك، يتسبب أيضًا استخدام الحكومة الالكترونية في مخاوف أمنية معينة، مثل التهديدات السيبرانية وانتهاكات البيانات وضبط الوصول، وغيرها. تعد تقنية البلوكشين الخاصة المؤمنة واحدة من التقنيات التي يمكنها المساعدة في التخفيف من تأثير الضعف الأمني داخل الحكومة الإلكترونية. تتناول هذه الدراسة أداء نظام الهايبرليدجر فابريك ، وهي منصة بلوكشين خاصة، من خلال تحليل سيناريوهين يتضمنان اضافة ست مؤسسات حكومية كدراسات حالة تحت معدلات ارسال عالية . تم تعديل عدة معاملات، مثل معدل إرسال البيانات وحجم كتلة البلوكشين ووقت انطلاق البلوكشين وعدد المؤسسات وعدد المستخدمين في كلا السيناريوهين. كما تم ايضا إضافة تدريجية للمؤسسات لتحديد تأثير زيادة عددها على إنتاجية النظام وتأخير وقت معالجة البيانات وقابليته للتوسع. تم الحصول على نتائج مقبولة للأداء والتأخير عند زيادة حجم البلوكشين إلى حوالي المئة معاملة لكل بلوكشين. ايضا تمت ملاحضة انه عند اضافة عدد من المؤسسات يصل الى ثلاثة فقط فأن النتائج تكون مقبولة في معظم الحالات ، لكن عندما تم إضافة المزيد من المؤسسات، بدأت الإنتاجية والتأخير تعاني من أداء ضعيف. كما أظهرت العديد من التجارب أن زيادة وقت البلوكشين لمعدلات الإرسال العالية كان له تأثير جيد على الإنتاجية والتأخير.