Performance Evaluation of Multi-Organization E-Government Based on Hyperledger Fabric Blockchain Platform

Osama I. Kadhum*, Ali H. Hamad

Department of Information and Communications Engineering, University of Baghdad, Baghdad 10070, Iraq

Corresponding Author Email: ooosaamaa84@gmail.com

ABSTRACT

E-governments can face various security problems due to the nature of online systems and the sensitive information they handle. Some of these security issues include: cyberattacks, data breaches, Identity theft, access control, and many others. Permissioned blockchain is one of the cutting-edge technologies that can help to reduce the impact of security vulnerabilities of e-governments. In this work, six organizations as a case study have adopted, two scenarios performed to analyze the performance of hyperledger fabric (a permissioned blockchain platform). In these two scenarios, several parameters have changed, including: transaction send rates, block sizes, number of organizations, and number of clients. The organizations have added gradually to conclude the effect of multi-organization on the throughput, latency, and scalability of the system. Good throughput and latency results were obtained by increase the block size to about 100 transactions per block. Within three to four organizations, the throughput and latency results were accepted, but adding more organizations, the throughput and latency have been affected negatively. Also, it has concluded that with few users in the system, the throughput and latency were reasonably good. Still, with adding more clients, the throughput decreased, and the latency increased rapidly.

1. INTRODUCTION

Due to the continuous advancement of information and communication technology (ICT) that has made interconnected and globally accessible organizations increasingly affordable, individuals can now rely on what is known as e-governments [1, 2].

The importance of e-governments cannot be overstated, as they have numerous benefits for both governments and citizens. Firstly, e-governments can improve the efficiency and effectiveness of government services. By digitizing government processes and services, eliminate paperwork, and streamline service delivery. This can save time and money, and make government services more accessible to citizens [3]. Secondly, e-governments can increase transparency and accountability. By making government information and data available online, citizens can have greater access to information about government policies, budgets, and decision-making processes. This can increase trust in government institutions and improve the quality of democratic governance [4, 5]. Thirdly, e-governments can empower citizens to participate in government decision-making. By providing online platforms for public consultation and feedback, e-governments can give citizens a voice in government decision-making processes, and facilitate citizen engagement in civic affairs [6]. Fourthly, e-governments can enhance cybersecurity and data privacy. By implementing robust cybersecurity measures and data protection policies, e-governments can protect citizens' information from cyber threads [7].

There are primarily four different kinds of interactions between the community and the e-government: Government to People/Citizens, Government to Government, Government to Business, and Government to Workers/Employees (G2C, G2G, G2B, and G2E) [8]. As shown in Figure 1.
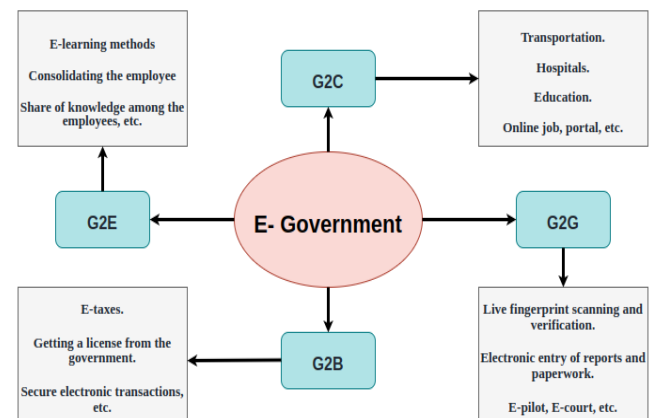
Figure 1. Types of e-government [4]

The public ought to have confidence in their government as well as in the technology they employ. Individuals frequently worry about the safety and privacy of their personal information. Yet, due to risks to the security and privacy of the e-government, public trust is lost, which is one of the reasons why citizens avoid using e-government systems. It is well known that if an e-government system is not adequately protected, it can have series consequences for citizens and the government, security assaults could damage it at any time and cause a variety of monetary, psychological,

and emotional losses [9].

Malware attacks, unauthorized access, theft of sensitive information, insider threads, and distributed denial of service (DDoS) attacks are common security vulnerabilities that could affect e-governments [10, 11]. E-governments security can be enhanced through the use of various technologies. Some of these technologies include: Encryption, multi-factor authentication, artificial intelligence and machine learning, cloud computing, intrusion detection and prevention systems (IDS and IPS), as well as blockchain technology [12].

Blockchain, which refers to a chain of blocks, where each block contains a record of transactions and a unique cryptographic hash of previous block [13, 14], can play a significant role in enhancing e-governments security by providing a secure, transparent, and tamper-proof platform for storing and sharing information [15]. Blockchain can be used to create a decentralized, tamper-proof digital identity system that verifies the identity of citizens and government officials. This system can help prevent identity fraud and ensure that only authorized individuals access government services [16]. Also, blockchain can be used to store sensitive government data, such as financial data or classified information, in a secure manner. This ensures that the data is protected from unauthorized access and manipulation. Smart contracts can be used to automate the execution of government services, ensuring that they are delivered in a secure, transparent, and efficient manner [17].

The idea of cryptocurrencies, particularly Bitcoin and Ethereum, which rely on permissionless networks, was what gave rise to the blockchain. Everyone can access the network and participate in the network using permissionless blockchains. Contrarily, permissioned blockchains are closed (not publicly accessible), meaning that only users with permissions can access them. These blockchains are ideal for many e-government applications, including: e-voting systems, banking transactions, health care, and much more [18].

The motivation behind this work is to address the challenges in the implementation of e-government systems that involve multiple organizations by leveraging the security, transparency, and scalability offered by the Hyperledger Fabric blockchain platform. Our goal is to provide a comprehensive performance evaluation of such a system to assess its performance and scalability feasibility and potential for improving e-government services.

In this work, the impact of multi-organization and multi-client has been evaluated and analyzed in the hyperledger fabric platform by measuring essential parameters such as average latency, throughput, and scalability each time the number of organizations as well as the number of clients increased. Key variables such as block size, number of concurrent transactions, number of clients, and number of organizations are modified to assess the platform's performance. The hyperledger caliper benchmark is utilized for this performance evaluation. Two main scenarios were conducted in this work. It was concluded that the performance of the blockchain network is influenced by hardware and software configuration, smart contract complexity, user and organization volume, and network architecture. It was also concluded that little number of organizations or clients or both have positive impact on the performance of the fabric platform, but increasing number of organizations or number of clients or both have contributed a lot in reducing the throughput of the entire platform as well as increasing the average latency, especially when both organizations and clients were increased.

The remainder of this paper is structured as follows: A collection of relevant works in the performance assessment of blockchain platforms is introduced in Section 2 of this article. section 3 talks about the history of the hyperledger fabric project. The multi-organizational system architecture was proposed in Section 4 included a variety of tests and scenarios. Lastly, section 5 describes the conclusion.

2. RELATED WORK

Recently, many researchers have been focusing their attention on the analysis of blockchain due to the significant role it plays in the creation of new algorithms. Saeed et al. [19] discussed the effect that the workload of electronic voting has on the hyperledger fabric framework including many parameters like latency and performance. The caliper tool was used in that test. Numerous different situations were tested by adjusting the transaction transmission speeds, block sizes, timeouts of the block, and the organizations simultaneously. Tanwar et al. [20] conducted research to determine the impact that a permissioned blockchain based on the hyperledger fabric platform would have on a modern healthcare system known as an electronic healthcare record (EHR) sharing system. This system employs the idea of a chaincode. They also used the caliper to measure significant parameters including, latency, throughput, block size, endorsement policy, block generation time, etc. to show the efficiancy of the EHR system. Their experiments provided insights into the hyperledger fabric transaction rate, throughput, and latency. Hang and Kim [21] proposed an innovative construction technique for a blockchain network in order to improve the hyperledger fabric efficiancy by analyzing several adjustable network topologies. Kuzlu et al. [22] discussed the effects of the performance of the blockchain architecture in many cases including scalability, latency, and throughput. In the simulated environment, multiple scenarios were tested by altering the rates of transaction, the parallel transactions number, and the transactions kind. Fan et al. [23] offered a thorough survey covering existing blockchain performance evaluation methodologies and suggested a number of enhancements. These ranged from system level optimization to more efficient consensus algorithms. These can be broken down into the empirical and analytical evaluation approaches from a high level perspective. Swathi and Venkatesan [24] offered a private blockchain as a solution to the problem of scalability by incorporating techniques from distributed machine learning. They included these techniques in the hyperledger fabric to evaluate the performance and latency of the system. Moschou et al. [25] came up with a mechanism for comparing and contrasting the capabilities of two distinct transaction processors that were integrated into the Hyperledger Sawtooth platform. They conducted an experimental evaluation of the technique, and they give the findings of the experimental evaluation, which may prove helpful to blockchain practitioners in the design of future solutions. Praveen M. Dhulavvagol et al. [26] refined the examination of the two well-known Ethereum clients, Geth and Parity. Time, consistency, and scalability considerations were taken into account when doing this investigation.

Saeed et al. [19] and Tanwar et al. [20] were the nearest to our work, as they engaged up to three organizations with few clients. But what distinguished our work is that we tried to engage more organizations (up to six) and more clients (up to

200) in the fabric platform to prove the scalability and performance of the system.

3. HYPERLEDGER FABRIC PLATFORM

Hyperledger is an open-source project created by the Linux Foundation to develop a suite of blockchain-based tools and frameworks for building enterprise-grade, permissioned blockchain networks. The goal of hyperledger is to provide a collaborative and neutral platform that can be used by developers and businesses to create blockchain-based solutions for a wide range of industries. Hyperledger has several sub-projects, including Fabric, Sawtooth, Burrow, Indy, and Iroha. These projects provide a range of blockchain frameworks and tools that can be used to build secure, scalable, and interoperable blockchain-based applications [27].

Hyperledger fabric is the most widely used project within the Hyperledger ecosystem, it was designed to meet the needs of enterprise applications by providing features such as permissioned access, high scalability, confidentiality, and flexibility. Hyperledger fabric uses a modular architecture that allows users to customize their blockchain networks based on their specific requirements [28].

Hyperledger fabric consists of various major components including: peer nodes, ordering service, ledger, chaincode, membership service provider (MSP), channels, fabric software development kit (SDK), and fabric certificate authority (CA). Figure 2 illustrates the transaction flow diagram of the hyperledger fabric [29]. The peer nodes are nodes in the network that maintain a copy of the ledger, execute chaincode, and validate the transactions. The ordering service is responsible for ordering and packaging the validated transactions into blocks and then broadcasting them to the peer nodes for validation and commitment to the ledger. The chaincode (also called smart contract) is a program that is deployed on a hyperledger fabric network and is responsible for handling transactions between network participants. it is written in many programming languages such as Go, Java, or JavaScript. The MSP is responsible for managing identities in the network, which includes registering new identities and authenticating users who want to interact with the network. A channel is a private sub-network that allows for secure communication between a subset of network participants. The fabric SDK provides developers with a set of APIs to interact with the hyperledger fabric network. The SDK is available in various programming languages such as Node.js, Java, and Python. The CA is responsible for issuing and revoking digital certificates for network participants. These certificates are used for authentication and authorization in the network [30].

There are two types of validation system chaincodes in Hyperledger Fabric, VSCC (Validation System Chaincode), which validates that the transaction has been signed by the correct set of peers according to the endorsement policy defined in the chaincode [31]. If the transaction is valid, the VSCC marks it as valid and forwards it to the ordering service for block inclusion. MVSCC (Multi-Version Concurrency Control Validation System Chaincode) which extends VSCC by adding support for validation of transaction endorsements in a multi-versioned chaincode environment. it validates that the transaction has been endorsed by the correct set of peers according to the endorsement policy of the chaincode version being executed. If the transaction is valid, the MVSCC marks it as valid and forwards it to the ordering service.
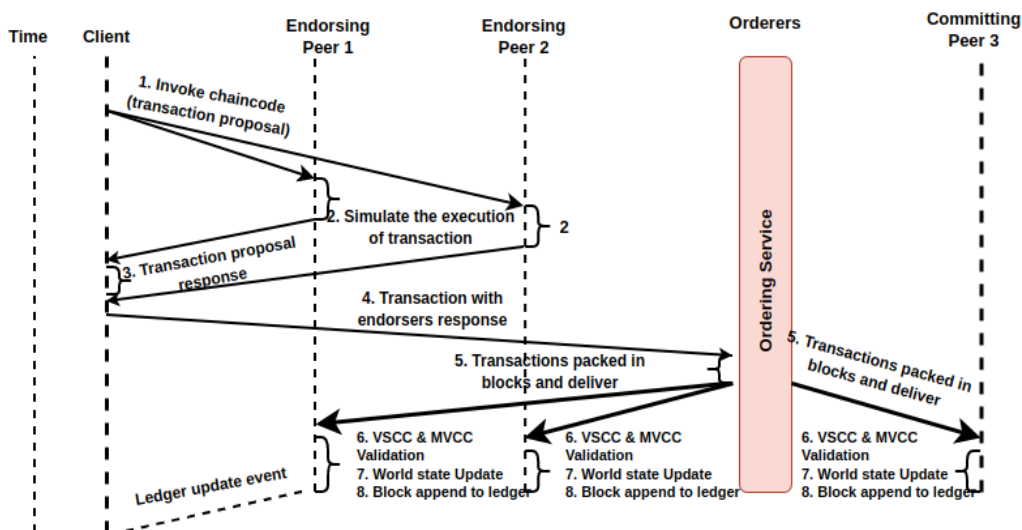

Figure 2. Transaction flow in hyperledger fabric

4. PROPOSED MUTI-ORGANIZATION SYSTEM DESIGN

In order to analyze the influence of blockchain workloads on the performance of the recent version of hyperledger fabric with long-term support, v2.4, a case study is presented in this article that uses six companies communicate with one another (that is, transmit transactions to one another). Client apps are able to communicate with all members of the proposed fabric network thanks to Fabric SDK. Members of the fabric network are represented by the committer, endorser, and orderer nodes. As can be seen in Figure 3, each organization possesses both a CA and an MSP. To grant certificates to its members and that stores the identities that have been granted permissions.

The purpose of performance assessment is to comprehend the performance of the system being assessed and to document that understanding. In this work, the performance of the system and its many characteristics are verified and tested

using hyperledger caliper, a tool that supports several hyperledger platforms, including Fabric. These parameters include latency, throughput, scalability, and other metrics that are required for the evaluation of the system. The assessment results are used to alter the configuration parameters, which include the number of transactions per second (tps), the number of clients, the number of organizations, and the block size, among other things. Some of the important configuration parameters are shown in Table 1. Transaction throughput and average latency are the two measures that have been monitored in two different monitoring scenarios involving six different companies. There has been some thought given to transaction rates of 50 tps, 100 tps, 150 tps, and 200 tps. Clients in increments of 10, 50, 100, 150, and 200 were included, and they were from five diverse categories. Transactions in the system are generated by the clients. Upon verification of the transactions, the network will add new blocks to the distributed ledger known as the blockchain.
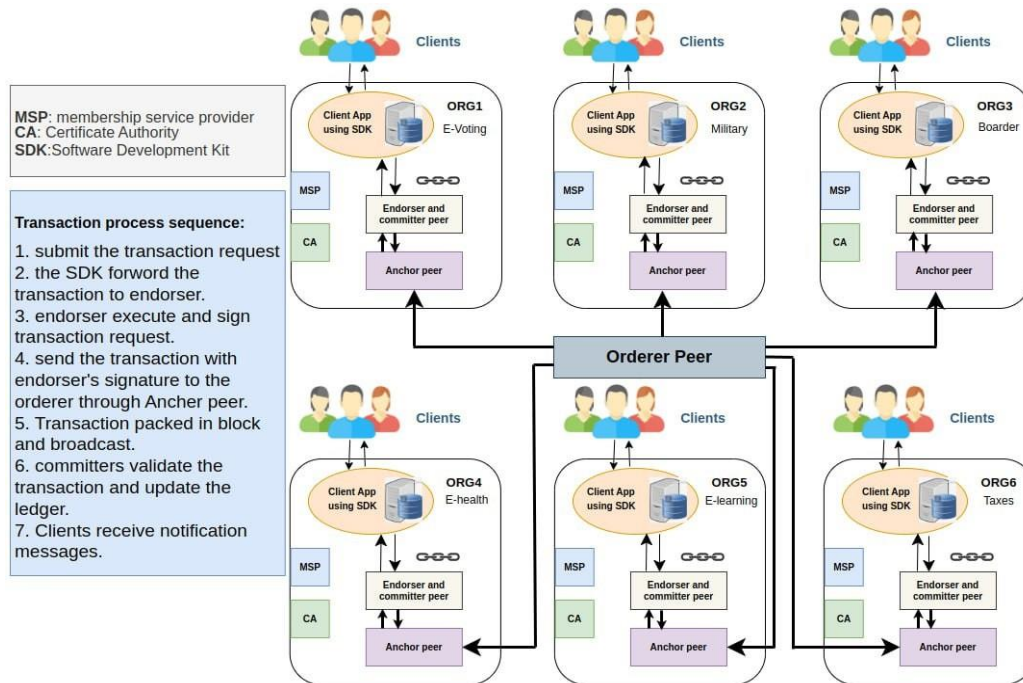

Figure 3. The architecture of the proposed multi-organizations system based on hyperledger fabric

Table 1. Important configuration parameters

Components	Description	Values
Block size	Maximum limit to fill up the block with transactions.	10, 50, 100, 150, and 200 (tx/block)
Batch timeout	The amount of time to generate a new block.	2 seconds (default)
Orderers	A node performs ordering services.	Raft
Endorser peers	Make approval to a transaction when it is proposed	1, 2, 3, 4, 5, 6
Programming languages	smart contract programming languages.	Node.js
Clients	the entities that interact with the system.	10, 50, 100, 150, 200
Organizations	A member that is invited to join the blockchain network.	1, 2, 3, 4, 5, 6
Ledger	The database used by the fabric to store transactions.	CouchDB
Send Rate	Measured in transactions per second.	10, 50, 100, 150, 200 TPS

4.1 Scenario 1: Increasing the send rates of the blockchain

In this scenario four rounds have been proposed to measure the throughput and average latency of the fabric platform, ten thousand transactions are included in each round. In all rounds the number of transactions per block was set to 10, each round with one specific TPS ranging from (10, 50, 100, 150, 200). Figures 4(a) and 4(b) show that when the transactions are set to 10 TPS, the throughput and average latency will remain constant even with increasing the number of clients from 10 to 200 and number of organizations from 1 to 6, with highest throughput was about 11.7 TPS at 200 clients for one organization. Figures 4(c) and 4(d) show that with increasing the transactions to 50 TPS, the throughput starts to decrease and the average latency starts to increase especially with increasing the number of clients and increasing the number of organizations, the highest throughput obtained was when number of clients are set to 10 at 4 organizations (about 40.5 TPS), and lowest throughput obtained when the number of clients increased to 200 at 6 organizations (about 7 TPS), also minimum latency obtained was when the number of clients were 10 at one organization (about 5 seconds) and maximum latency obtained at 200 clients and 6 organizations (about 26 seconds). Figures 4(e), 4(f), 4(g), and 4(h) show a dramatic decrease in throughput and dramatic increase in average latency with increasing the transactions to 150 and 200 TPS especially with increasing the number of clients in the system and the number of organizations, the lowest throughput and highest latency obtained was at 6 organizations with 200 clients and 200 TPS (about 3.5 TPS and 50 seconds). The reason behind the decreasing in throughput and increasing the average latency with the increasing of number of organizations and / or increasing of number of clients is the increasing in number of endorsements each time a client sends a transaction.

## 4.2 Scenario 2: Varying the block size of the blockchain

In this scenario four rounds have been experimented to measure the throughput and average latency. Every round is set with 10000 transactions. In all rounds the send rate is set to 100 TPS while increasing the block size each round from (10, 50, 100, 150, 200) transactions per block. Figures 5(a), 5(b), and 5(c) show that when we increase the size of the block from 10 to 50 and 100 transactions in each block, the throughput begins to increase over all organizations, as an example at block size=10 the highest throughput at six organizations with 100 clients was about 30 TPS, and at block size=50 the maximum rate was around 37 tps, whereas at size of block=100 the highest throughput increased to about 44 TPS. Figures 5(d) and 5(e) show that with the block size being increased to include more than 100 transactions per block, i.e. reaching 150 or 200 transactions in each block, the throughput

either remains constant or starts to decrease slightly especially with the increasing the number of clients and organizations. This experiment also showed as in Figure 6(a), 6(b), 6(c), and 6(d) that when the size of the block has increased from 10 to 50 and 100 transactions, the latency has decreased especially with the first three organizations, while increasing the size of the block to 150 and 200 transactions as shown in Figures 6(e) and 6(f), made the latency starts to increase especially with the increasing of number of organizations and number of clients. The experiment implies that increasing the size of block to more than 100 transactions per block has no benefit to the performance, also it is noted from this experiment that better performance and latency obtained from smaller block sizes which is about 50 transactions in each block. Hence, raising the block sizes by a significant amount had little effect on performance.

(a)

(b)

(c)

(d)

(e)

(f)
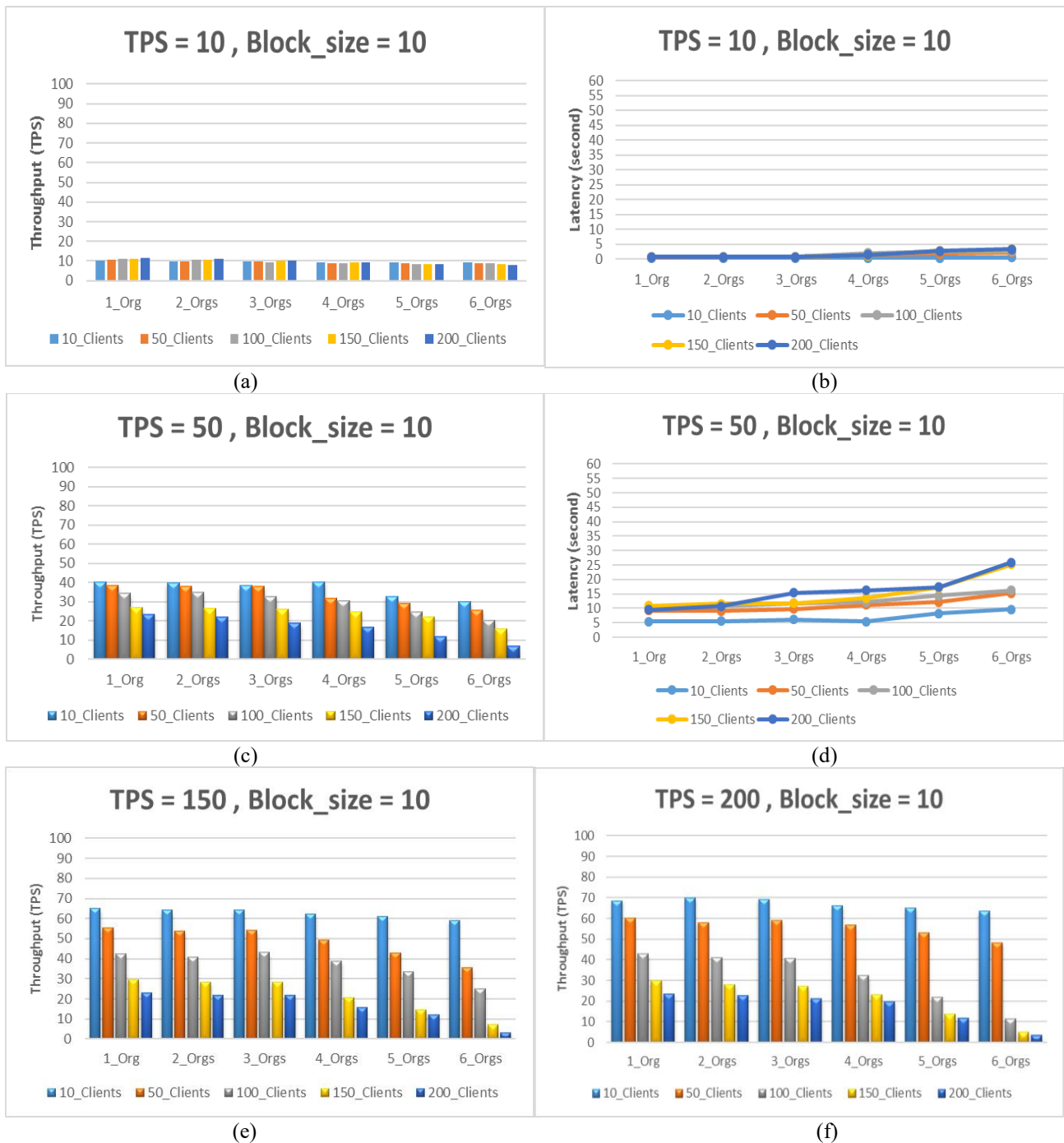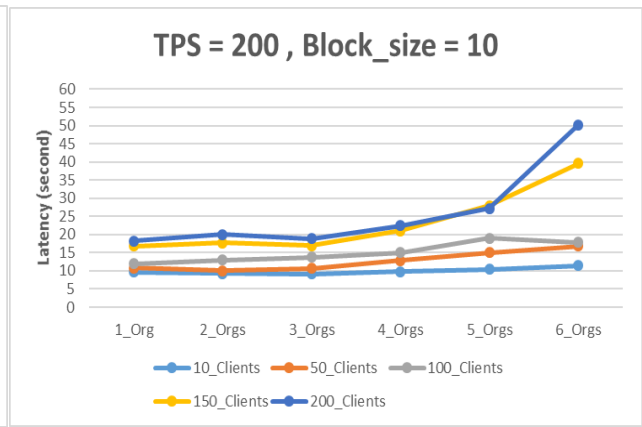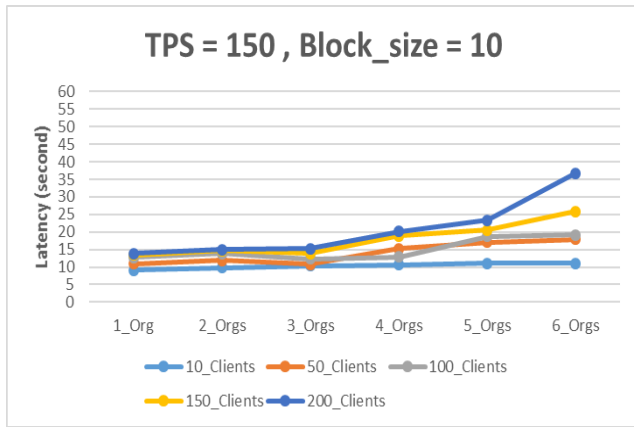
(g)

(h)

Figure 4. Throughput and latency results of varying the send rate in TPS
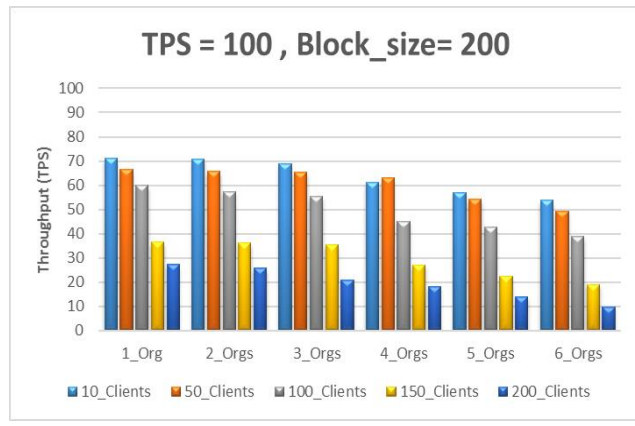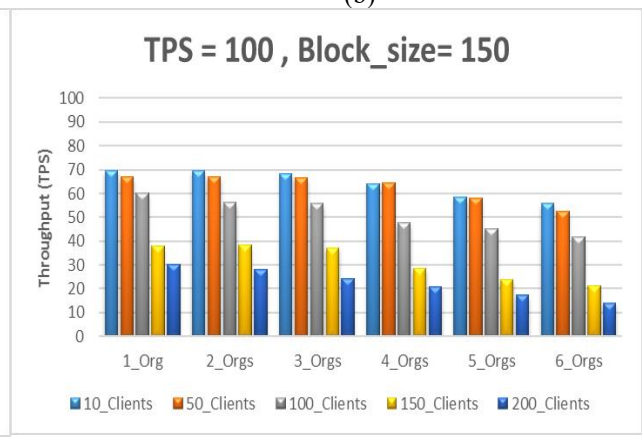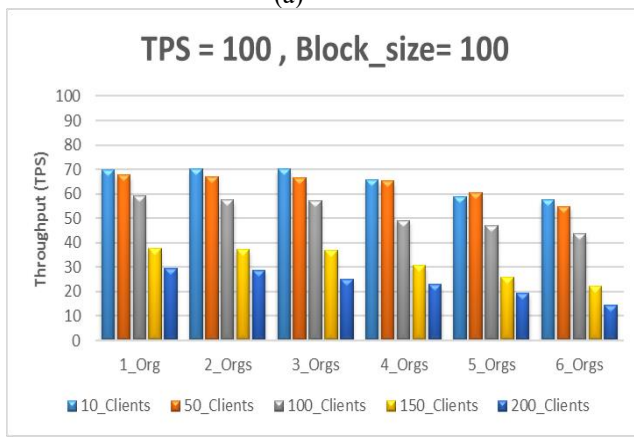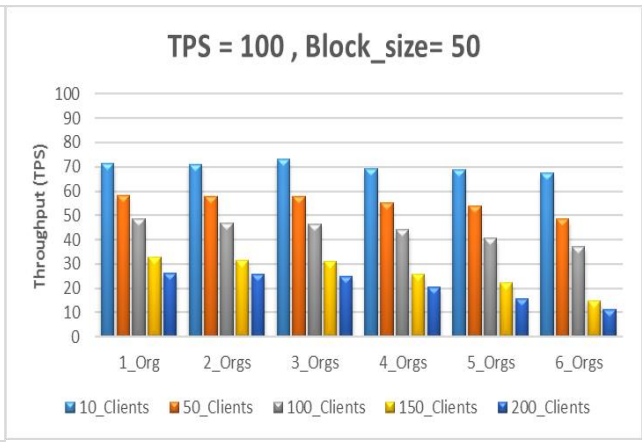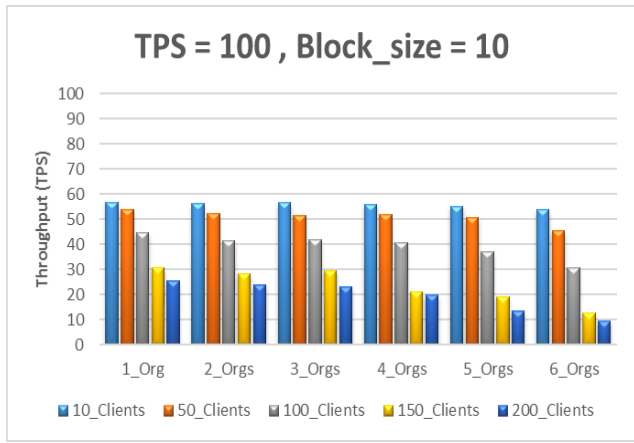
(a)

(b)

(c)

(d)

(e)

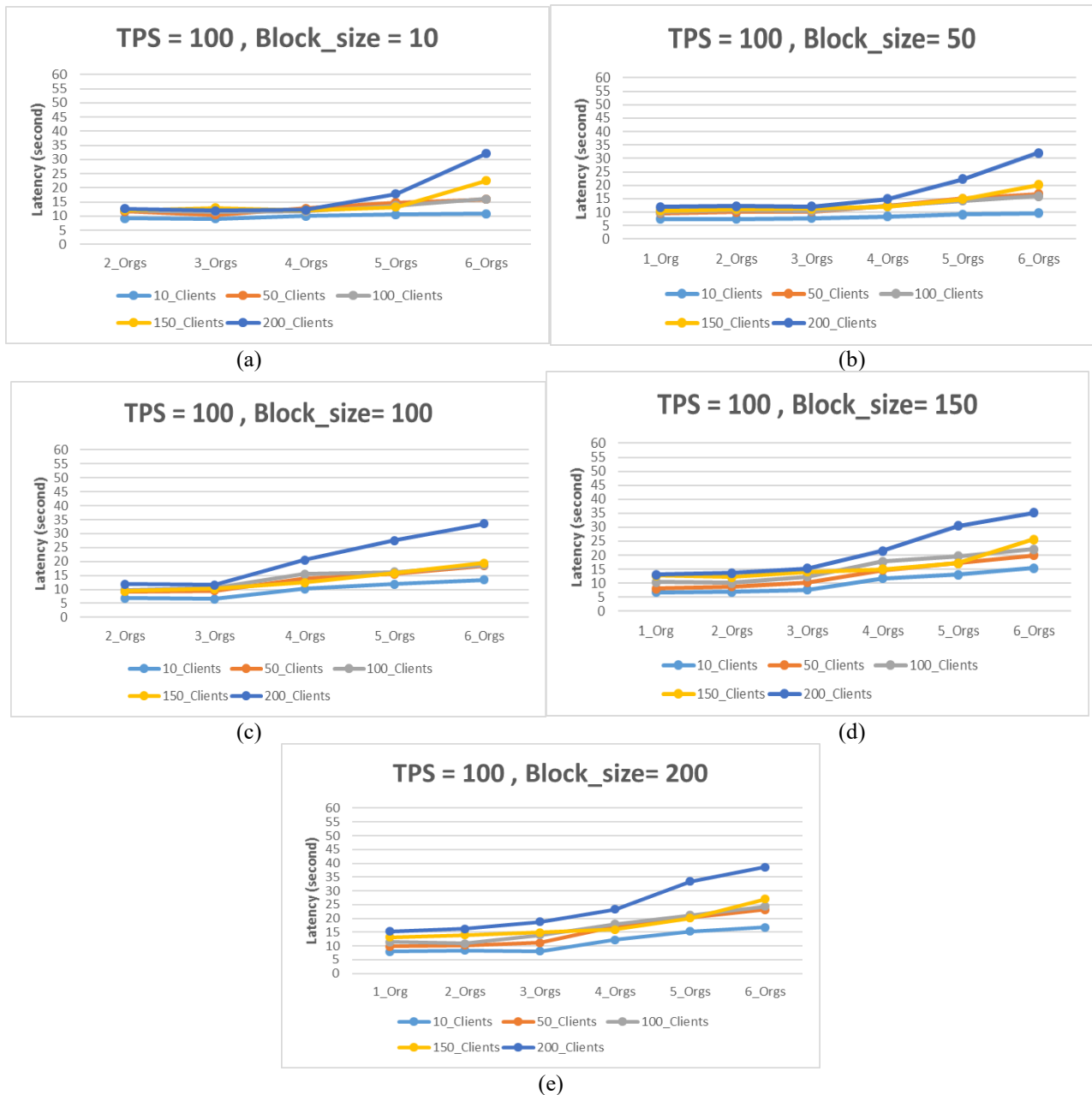**Figure 5.** Throughput results of varying block size

504

Figure 6. Latency results of varying block size

5. CONCLUSIONS

This work examined the multi-organization impact with an increasing number of clients on essential parameters such as throughput, latency, and scalability of the hyperledger fabric blockchain platform. Two scenarios were run by adjusting several significant factors, like, the transaction transmits rates (tps), block sizes, and client and organization counts. In conclusion, the fabric blockchain platform depends on the hardware and software configuration, the smart contracts' complexity, the number of clients engaged with the system, the number of linked organizations, and the network design. Thus, the following findings were drawn in further detail:

1. we found that the throughput and latency performance of the fabric blockchain platform is strongly impacted by the transaction rates, number of organizations, and the clients engaged in the system. Such that, when the transaction rate was set to 10 (tps), which is considered low, throughput and latency performance was at optimum conditions as they remained approximately constant even with increasing the organizations or the clients or both. But, by increasing the transaction rate to 50 and 100 (tps), the system's performance was degraded gradually, especially with the increased number of organizations and engaged clients. System performance experienced a significant drop when the transaction rates rose to 150 and 200 (tps), especially when entering more clients into the system (about 200 clients).

2. Setting the size of the block to about 100 (transactions per block) had a better effect on the throughput and latency of the system. It gave better results as compared to other block sizes, even with a higher number of users engaged.

3. Good throughput and latency results were obtained with the first three to four organizations, especially with a moderate number of active clients. On the contrary, low performance and high latency were reached by involving the fifth and sixth organizations, especially with increasing the number of clients, and that's because of the increase in the number of endorsements in the network.

4. To minimize latency in time-sensitive transaction applications, it is preferable to employ smaller block sizes. This is because smaller block sizes, although they suffer from low throughput, but take less time to fill the block with data, which reduces latency.

5. In this work, as compared to previous works, we tried to engage more organizations (up to six) and more clients (up to 200) in the fabric platform and discover the impact of that increase on the overall system in terms of throughput, average latency, and the scalability. Most previous studies engaged less number of organizations (up to 3) and less number of users, and this is good. But to adequately clarify this platform's performance, it was necessary to add more organizations and more clients. And that is what we did in this work.

6. This article can contribute significantly to the study of hyperledger fabric platform in several ways: Firstly, the evaluation can provide insights into the strengths and weaknesses of existing e-government systems and identify areas for improvement. This information can help policymakers and stakeholders to make more informed decisions when developing new systems or upgrading existing ones. Secondly, the evaluation can help identify the most efficient configurations and parameters for blockchain-based e-government systems, including network topology, consensus mechanism, and transaction validation process. This can help to optimize the performance and scalability of these systems. Finally, the evaluation can help identify security vulnerabilities in e-government systems and suggest ways to mitigate them. This is particularly important in the case of blockchain-based systems, which are often touted for their security benefits but can still be vulnerable to attacks.

7. Our findings demonstrate the applicability of this work, with particular emphasis on addressing the critical aspect of scalability in the fabric platform. The scalability of this platform is crucial for its effective deployment across various e-government applications, thereby potentially yielding significant impact.

ACKNOWLEDGMENT

REFERENCES

[1] Stoica, M., Ghilic-Micu, B. (2020). E-government in Romania–A case study. Journal of E-Government Studies and Best Practices, 2020: 608643, http://dx.doi.org/10.5171/2020.608643

[2] AL-Ghraibawy, A.M.K. (2022). 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. Journal of Economics and Administrative Sciences, 28(131): 59-82. https://doi.org/10.33095/jeas.v28i131.2234

[3] 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

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

[5] Hayder, I.M., Younis, H.A., Abed, I.A., Younis, H.A. (2020). 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, pp. 117-121. http://dx.doi.org/10.1109/IICETA50496.2020.9318959

[6] Shin, S.C., Ho, J.W., Pak, V.Y. (2020). Digital transformation through e-Government innovation in Uzbekistan. In 2020 22nd International Conference on Advanced Communication Technology (ICACT), pp. 632-639. http://dx.doi.org/10.23919/ICACT48636.2020.9061507

[7] Cho, S.H., Oh, S.Y., Rou, H.G., Gim, G.Y. (2019). A study on the factors affecting the continuous use of E-Government Services-Focused on privacy and security concerns. In 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 351-361. http://dx.doi.org/10.1109/SNPD.2019.8935693

[8] Khoirul Aswar, R., Sumardjo, M., Wiguna, M., Hariyani, E. (2022). Personal and reliability factors affecting adoption and utilization of e-government: An effect of intention to use. Problems and Perspectives in Management, 20(2): 281-290. http://dx.doi.org/10.21511/ppm.20(2).2022.23

[9] Nguyen-Duc, A., Do, M.V., Hong, Q.L., Khac, K.N., Quang, A.N. (2021). On the adoption of static analysis for software security assessment–A case study of an open-source e-government project. Computers & Security, 111: 102470. https://doi.org/10.1016/j.cose.2021.102470

[10] Thompson, N., Mullins, A., Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. Government Information Quarterly, 37(1): 101408. https://doi.org/10.1016/j.giq.2019.101408

[11] 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, 36(2): 233-240. https://doi.org/10.18280/ria.360207

[12] Ortiz-Lizcano, M.I., Arias-Antunez, E., Bravo, Á.H., Caminero, M.B., Guillen, T.R., Cha, S.H.N. (2023). Increasing the security and traceability of biological samples in biobanks by blockchain technology. Computer Methods and Programs in Biomedicine, 231: 107379. https://doi.org/10.1016/j.cmpb.2023.107379.

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

[14] Hassan, A.A. (2022). Blockchain technology and its potential effect on the banking industry (China Case Study). Journal of Economics and Administrative Sciences, 28(131): 133-149.

https://doi.org/10.33095/jeas.v28i131.2240

[15] Abdulhussein, A.B., Hadi, A.K., Ilyas, M. (2020). Design a tracing system for a seed supply chain based on blockchain. In 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), pp. 209-214. http://dx.doi.org/10.1109/IICETA50496.2020.9318792

[16] Shalaby, S., Abdellatif, A.A., Al-Ali, A., Mohamed, A., Erbad, A., Guizani, M. (2020). Performance evaluation of hyperledger fabric. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 608-613. http://dx.doi.org/10.1109/ICIoT48696.2020.9089614

[17] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8: 79764-79800. http://dx.doi.org/10.1109/ACCESS.2020.2988579

[18] Prakash, R., Anoop, V.S., Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. International Journal of Information Management Data Insights, 2(2): 100112. https://doi.org/10.1016/j.jjimei.2022.100112

[19] 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.

[20] Tanwar, S., Parekh, K., Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50: 102407. https://doi.org/10.1016/j.jisa.2019.102407

[21] Hang, L., Kim, D.H. (2021). Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance. Blockchain: Research and Applications, 2(1): 100009. https://doi.org/10.1016/j.bcra.2021.100009

[22] Kuzlu, M., Pipattanasomporn, M., Gurses, L., Rahman, S. (2019). Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability. 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, pp. 536-540. http://dx.doi.org/10.1109/Blockchain.2019.00003

[23] Fan, C., Ghaemi, S., Khazaei, H., Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. IEEE Access, 8: 126927-126950. http://dx.doi.org/10.1109/ACCESS.2020.3006078

[24] Swathi, P., Venkatesan, M. (2021). Scalability improvement and analysis of permissioned-blockchain. ICT Express, 7(3): 283-289. http://dx.doi.org/10.1016/j.icte.2021.08.015

[25] Moschou, K., Theodouli, A., Terzi, S., Votis, K., Tzovaras, D., Karamitros, D., Diamantopoulos, S. (2020). Performance Evaluation of different Hyperledger Sawtooth transaction processors for blockchain log storage with varying workloads. In 2020 IEEE International Conference on Blockchain (Blockchain), pp. 476-481. http://dx.doi.org/10.1109/Blockchain50366.2020.00069

[26] Dhulavvagol, P.M., Bhajantri, V.H., Totad, S.G. (2020). Blockchain ethereum clients performance analysis considering E-voting application. Procedia Computer Science, 167: 2506-2515. https://doi.org/10.1016/j.procs.2020.03.303

[27] Al-Sumaidaee, G., Alkhudary, R., Zilic, Z., Swidan, A. (2023). Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. Information Processing & Management, 60(2): 103160. https://doi.org/10.1016/j.ipm.2022.103160

[28] Sun, Q., Yuan, Y. (2022). GBCL: Reduce Concurrency Conflicts in Hyperledger Fabric. In 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS), pp. 15-19. http://dx.doi.org/10.1109/ICSESS54813.2022.9930267

[29] The Linux Foundation Project. Available online: https://www.hyperledger.org, accessed on 4 March, 2023

[30] Ma, J., Jo, Y., Park, C. (2020). PeerBFT: Making hyperledger fabric's ordering service withstand byzantine faults. IEEE Access, 8: 217255-217267. http://dx.doi.org/10.1109/ACCESS.2020.3040443

[31] The official documentation of hyperledger fabric v2.4 available online, https://hyperledger-fabric.readthedocs.io/, accessed on 4 March 2023.