Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: Suppl. November 2022 **2022, 19(6): 1592-1602** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2022.7513

Proposed Framework for Official Document Sharing and Verification in E-government Environment Based on Blockchain Technology

Rana F. Ghani [1*] ***Asia Ali Salman Al-Karkhi*** [1] ***Shakir Mahmood Mahdi*** [2]

[1] Department of Computer Science, University of Technology, Baghdad, Iraq.
[2] Division of Graduate Studies, University of Technology, Baghdad, Iraq.
[*]Corresponding author: 110016 @uotechnology.edu.iq
E-mails address: asia.a.alkarkhi@uotechnology.edu.iq, shakir.m.mahdi@uotechnology.edu.iq.

Received 8/6/2022, Accepted 20/9/2022, Published Online First 25/11/2022, Published 5/12/2022

Abstract:

Progression in Computer networks and emerging of new technologies in this field helps to find out new protocols and frameworks that provides new computer network-based services. E-government services, a modernized version of conventional government, are created through the steady evolution of technology in addition to the growing need of societies for numerous services. Government services are deeply related to citizens' daily lives; therefore, it is important to evolve with technological developments—it is necessary to move from the traditional methods of managing government work to cutting-edge technical approaches that improve the effectiveness of government systems for providing services to citizens. Blockchain technology is among the modern technologies highly suitable for developing digital governance services, and its technological ability to sustain information stability is vital in digital governance systems since it improves integrity and transparency measures while preventing corruption. In this study, computer networking protocols are built to form a peer-to-peer network framework for managing official documents. using blockchain technology was built to illustrate how any element of government work may be developed using it. The suggested framework comprises the addition of a new official document, and the verification of an existing document. The system was created in socket programming using Java and tested the response times for many simultaneous requests. The system was tested using transactions per second (throughput) measurement. The result showed that the proposed system processed 200 document verification transactions within 50 seconds. In addition, the test of the proposed system presented the time required for document retrieval—about three seconds to answer 100 document retrieval transactions. Furthermore, the results of throughput were compared to the results of the same measurement of some popular applications such as bitcoin. And the result of the proposed system was within the average value of output throughput of the other compared applications.

Keywords: Blockchain Technology, Computer Network, Distributed System, E-government, Peer-to-Peer Network.

Introduction:

The continuous developments of computer networks take variant approaches of work. Some of works is focusing on improving existent technologies, other works focuses on developing novel technologies in computer network to allow for providing new types of services [1,2]. Virtually all elements of business and governmental work utilize the Internet or computer networks, and the digital transformation of these sectors has highlighted the importance of sharing sensitive and dangerous information safely. Although email, web applications, and the Cloud are commonly used to share information, relying on a third party to transmit data in particular applications may not be an option. As a result, the need to deploy a system that can be utilized to share data in a controlled and private manner has arisen. To fill this void, blockchain technology emerged as an Internet trust protocol. Apart from its capacity to share data in a controlled and privacy-preserving manner, blockchain includes immutable records of transactions among a network of nodes. The history of blockchain technology

started when Stuart Haber and W. Scott Stornetta described a chain of blocks using a hash function, digital signature, and time stamp for security in 1991; this was the birth of blockchain [3]. However, the greatest growth in blockchain technology was introduced by Satoshi Nakamoto as a secure framework to allow peer-to-peer Bitcoin transactions [4]. In 2014, blockchain 2.0 was introduced, which separated blockchain from bitcoins and allowed applications beyond cryptocurrencies. In this era, Ethereum and other platforms emerged and began implementing blockchain applications. Currently, decentralized file storage and decentralized autonomous group access are two examples of blockchain technology's application [5].

E-government is one industry that has benefited from the birth and advancement of blockchain technology. E-government refers to governmental agencies' use of information technology to improve the delivery of public sector services to citizens and improve the efficiency of government management [6]. The following are the key advantages of e-government [6-8]:

- Less corruption: Through e-government, government corruption vulnerability is reduced by increasing the monitoring capacity of stakeholders.
- Increased transparency: E-government improves transparency by providing wide monitoring coverage and collaboration with stakeholders.
- Greater convenience: E-government is a commitment to improving the satisfaction of citizens through the efficient delivery of services by governmental agencies. Citizens' satisfaction includes effective service costs in addition to increased responsiveness when delivering these services.
- Revenue growth: Government revenue increases when fraud and the shadow economy are reduced. The shadow economy includes economic activities that escape detection in official estimates, leading to reduced tax revenue and forcing governments to find other sources of revenue to finance public spending.
- Administrative burden reduction: Administration burdens have costs resulting from government-imposed legislation and regulation on businesses and citizens complying with their obligations.

The main challenges that face the implementation of e-government systems are [6]:

- Lack of general standards to implement e-government systems.
- The challenge of privacy invasion.
- Security threats.

In this paper, the work of administration departments in public and private sector institutions has been considered. The work of these departments focusses on archiving official documents, retrieving archived documents as needed, and the verification of the veracity and existence of documents. These services are vital for governmental work because they represent the bottleneck of the system if there are many requests at the same time. Usually, official documents contain information needed for other work, for example, you may request retrieval and verification of financial documents before using the information in these documents to create a report on the expenditures of the institutions during a period of time. The query related to the existence and veracity of the financial documents must be answered very quickly in order to proceed with writing the required report.

In this work, development of a general framework to improve e-government services by using blockchain technology has been presented. This work aims to digitally transform the work of administration departments. Two typical services offered by most government agencies' administration departments and used a blockchain system to reformulate them were looked at: 1- Storing official letters in a blockchain system and 2- Verifying the veracity of these documents. Although there are a number of archiving systems, such as Amazon S3 Glacier and Microsoft Exchange, these archiving applications participated the idea of using a third party to coordinate and control the flow of work of the administration and the management of official documents. The existence of a third party is considered a potential bottleneck and is contrary to the principle of transparency [9].

The main contributions of this work are as follows:

1. The design and implementation of a blockchain-based framework to share and manage official documents in a controlled manner.
2. The archival and the management of official documents without using a third party. This will add transparency to archiving systems.
3. Testing the effectiveness of using blockchain technology to implement an e-government system.

The suggested framework is assessed using two metrics: Firstly. throughput, which is defined as the number of completed transactions in a given amount of time, transactions are either request retrieving documents or verification of existence of a document. Secondly, the variation of the response of

the portal is also tested according to the increment in number of transactions.

The rest of the paper is organized as follows: Section 2 reviews related work in the blockchain domain, Section 3 briefly describes the background that were depended on to implement the proposed system, Section 4 introduces the proposed blockchain-based administration department in an e-government context, Section 5 describes our framework and results, and Section 6 is the conclusion and suggestions for future development.

Related Work

Many researchers have investigated the role of blockchain technology to improve aspects of e-government; here, some of these studies were considered. Cai and Zhu [10] focused on fraud detection and reduction and concluded that blockchain systems are effective for preventing fraud, especially loan application fraud. However, their effectiveness is limited in subjective information fraud where the truth is not easily validated. Hou [11] discussed the application of blockchain technology in e-government, particularly in a Chinese context. The article found that blockchain technology brings benefits such as improvements in government services and information-sharing across different organizations. However, security, cost, and reliability are still major problems in such applications. Therefore, he concluded that it is crucial to establish a platform to apply blockchain technology in e-government. Liu et al. [12] discussed the potential risk of privacy disclosure that citizens may face when their data is shared among government departments. They concluded that the use of blockchain to implement e-government services would enhance the security, credibility, and responsiveness of information sharing between departments and protect the privacy of citizens. Naiknavare et al. [9] suggested a blockchain-based solution to achieve transparency in nongovernmental agencies (NGOs). The aim of the proposed solution is to ensure trust between donors and NGOs. Ghani et al. [13] introduced a proposed framework for e-certification sharing using blockchain technology. Graduates, recruiting agencies, and universities around the world may be involved in this system. The system was evaluated for the average response time on a batch of transactions requesting the verification of students' e-certifications.

All these researchers have studied using blockchain technology by applying one or more features of the blockchain technology for e-government services. In this work, the work and services of the administration department in conventional governmental work have been studied and transformed digitally using blockchain technology, considering all benefits gained from the related work to improve the service of archiving official documents as well as all the services related to this work.

Background

This section presents the background used to implement the proposed administration department system in an e-government context using blockchain technology.

Blockchain Technology Concepts

Internet technology is constantly evolving, and the main direction of its evolution is decentralization. Therefore, blockchain technology is considered as the future internet. Blockchain is described as a distributed system to store information for a decentralized network [14]. Nodes in a blockchain network have a copy of the distributed ledger in addition to the facilities and skills to interpret the data and verify the data within the blockchain. The relation among nodes within a blockchain network is peer-to peer; they do not rely on a trusted third party. Each node examines a received transaction and decides to either commit that transaction to its copy of the ledger, depending on the consensus scheme, or to reject it. When a block is mined using a consensus scheme, this new block is broadcast to all the nodes within the blockchain network. The nodes will then commit it to their copy of the ledger [15]. Each block consists of two parts: A header and the data. The header consists of various fields, depending on the construction platform and the application itself. Typically, the header has a cryptographic hash of the previous block in the chain, the root hash of the Merkle Tree, the time stamp, the goal of the current difficulty, and the nonce (a four-byte field that usually starts with zero). The data part of the block contains the transactions. The predetermined block and transaction sizes determine the maximum number of transactions within a block [16].

The Merkle Tree is an intrinsic component of blockchain; it is a hierarchical data structure that enables the secure verification of data collections and is used to organize a large amount of information and to verify this information efficiently and quickly. The Merkle Root is used to accelerate transaction verifications and to check for the existence of a specific transaction in a certain block [17- 19].

A consensus algorithm is a protocol through which all parties in a distributed computing environment agree on a single data value. It is an essential element in blockchain and is used to guarantee the integrity and security of the data in the distributed ledger. Consensus algorithms are

categorized into two types [20]: Proof-based and vote-based consensus algorithms. In the first type, nodes should prove that they have performed sufficient verifications to obtain the right to do the transaction, thereby adding work to the ledger and getting the rewards. In the second type, messages are exchanged among the nodes in order to agree on the blocks or transactions to be added to the ledger [21]. The blockchain framework is illustrated in Fig. 1.

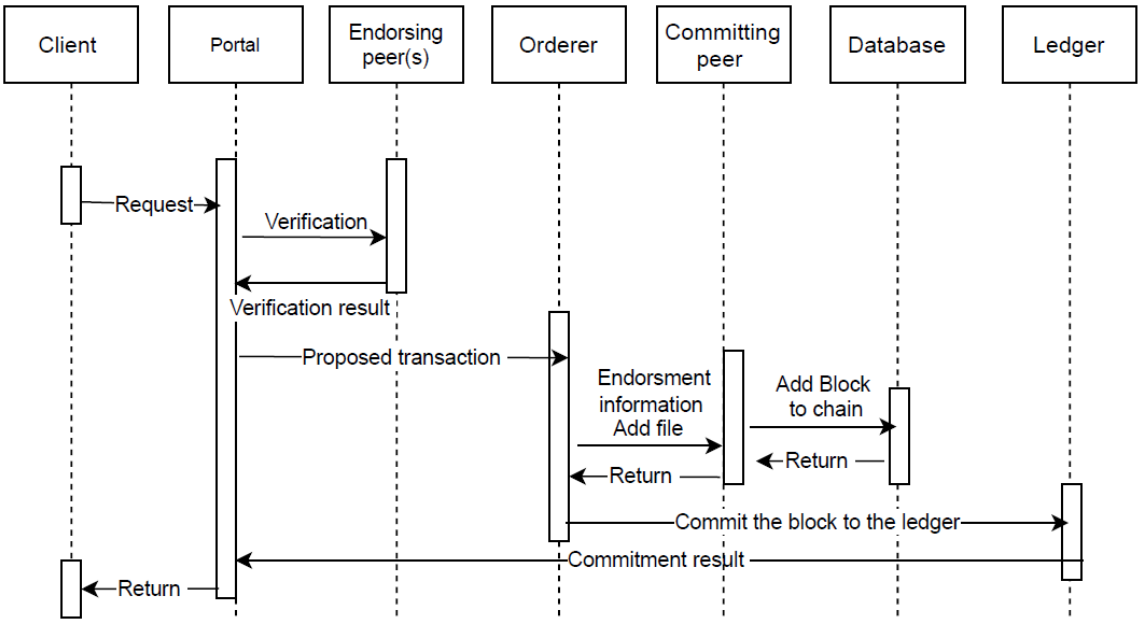

Figure 1. Blockchain general framework

Smart Contracts

Smart contracts are considered the digital form of traditional contracts. They are usually stored on a blockchain and can self-execute if the entities of the contract have met the predetermined terms and conditions of the contract [22]. In addition, it is a predetermined contract that is provable without the need for a trusted party [17]. Entities depend on the conditions and terms of the smart contract to enter into the agreement determined by the contract. Since the contract terms are transparent to these entities, they ensure the integrity of the contract, and they would be able to check the immutability of the blockchain and no party will alter the conditions and terms of that contract in the future. Blockchain-based applications reap huge benefits from using smart contracts [22]:

1. High throughput and efficient and accurate work due to the immediate execution of the digital contract when the terms are met.
2. High transparency and security because a peer-to-peer protocol to share encrypted transaction records is used. Additionally, each record is connected to the previous and subsequent records on a distributed ledger; therefore, altering the content of a record would alter the entire chain.
3. Saving time and money because there is no need for a third party to handle transactions.

Blockchain Technology for E-government

Applying blockchain technology to e-government has many advantages, and e-government leverages the intrinsic features of blockchain technology. Therefore, the advantages of using blockchain technology to develop an e-government framework are as follows [23]:

- Allowing secure storage of government, citizen, and business data.
- Allowing controlled information sharing.
- Reducing management costs for process auditing.
- Reducing potentials of corruption and abuse.
- Eliminating third parties.
- Increasing trust in government and online services.

While blockchain has many specifications that make it promising as an efficient framework for e-government, there are challenges that could exploit blockchain in e-government, such as the following:

- It is an emerging technology.
- It lacks experts and policies.
- It is ambiguous when it comes to scalability and interoperability.

The Work of Administration Departments in Government Institutions

The main task of the administration department in any government institution is to issue and archive official letters, retrieve them upon request, and provide relevant parties with a copy. Therefore, it is the responsibility of the administration department to issue, document, and preserve the official letters in a way that prevents any future changes to and falsification of them. The traditional tasks of the administration department are as follows:

A. The process of issuing official letters according to the following stages:
   a) Typing official letters.
   b) Sending official letters to the director of the governmental institution for signing.
   c) Providing official letters with numbers and dates.
   d) Issuing official letters.
   e) Archiving the letters in the administration department.

B. The process of verifying an official letter happens when a certain party needs a specific letter that was previously issued. This includes the following stages:
   a) Submitting a request to the administration department to obtain a copy of a specific official letter.
   b) Searching for the requested letter by an administrative department employee, depending on the document number and date or on the subject and content of the document.
   c) If the document exists, copying and providing it to the party that requested it.

Here, it is possible of documents being counterfeited and content changed because the sharing process of these documents is not subject to control or tracking after issuing multiple copies. In addition, there is the possibility of losing these documents due to weaknesses in the archiving system. Therefore, using blockchain technology has been suggested to issue, document, and control the sharing of official letters in governmental institutions.

Blockchain-Based System Evaluation Methods

Nowadays, many applications in various fields are implemented on the base of blockchain technology. The performance of these application depends on many factors, such as application criteria, size of the data, types of algorithms used within blockchain, and the type of blockchain. Therefore, it is difficult to determine a uniform measure for the quality of the blockchain-based application.

Most applications use the number of transactions per second to demonstrate the speed of transactions processing within application. Table. 1, shows some examples of numbers of transactions per second, and later, in the results section, these values will be compared with the same measurement for the proposed system [24].

Table 1. Examples of transactions per second for some blockchain-based applications [24]

Application Name	Number of Transactions per Second (Throughput)
Bitcoin (BTC)	7 TPS
Ethereum (ETH)	15–25 TPS
Litecoin	56 TPS
Bitcoin Cash (BCH)	250 TPS

The Proposed Framework for Blockchain-Based Official Letter Management

In the previous section, the tasks of official letter management in governmental institutions was explained. This section describes the proposed framework to do the same tasks in an e-government environment based on blockchain technology. The name of the proposed system will be abbreviated as FBCOLM. The blockchain-based framework considers two tasks: Issuing official letters and verification of official letters.

1. Issuing official letters: This task represents issuing official letters using blockchain technology. Fig. 2, shows that the framework of this task includes typing the letter by the client, the director of the institution as an endorser, and the employees of the administration department serving as the orderer and the committer. Additionally, the system includes a portal as a frontend for the system that is used to upload the typed letter.
2. Verification of an official letter: The second task in FBCOLM is to verify the validity of an official letter. If clients of the framework have been shared and would later like to verify the validity of the letter, then they must send a verification request for the letter. The portal of the framework receives the request and begins the verification task. If the letter exists in the blockchain, the client will receive a message verifying the validity of the letter; otherwise, the portal returns an invalid message. The verification task uses the hash value of the letter and makes a comparison with the Merkle Tree of the blocks within the ledger. The framework of the verification task is shown in Fig. 3.

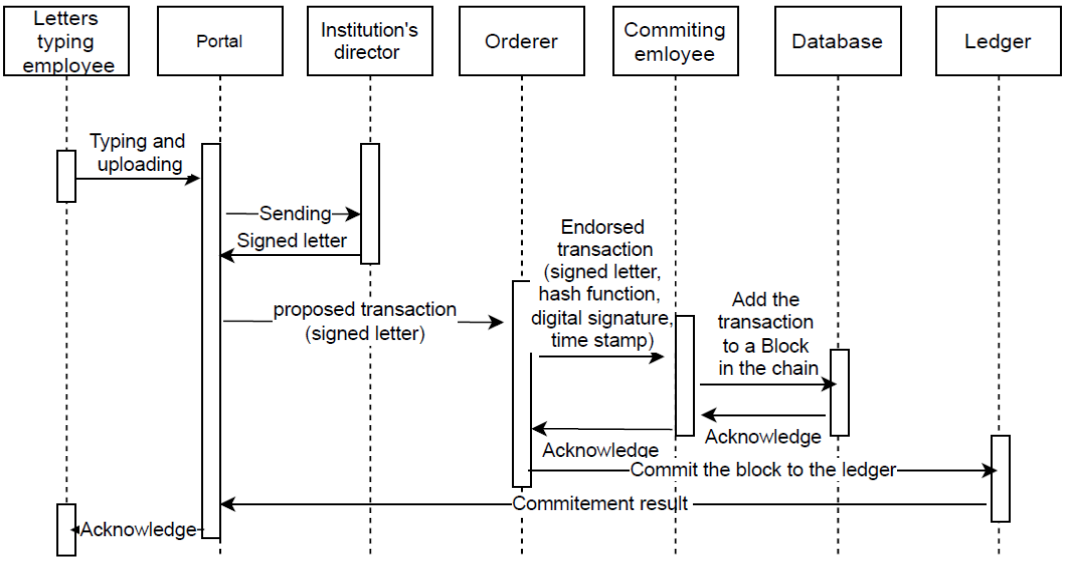

Figure 2. Issuing task framework

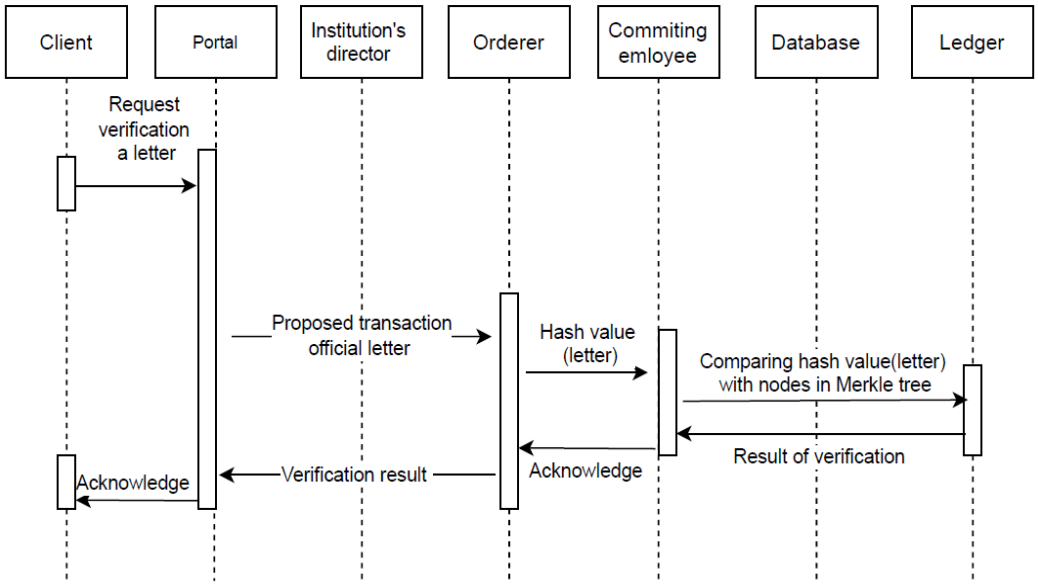

Figure. 3:Verification task framework

Issuing an official letter represents adding a new and trusted official letter to the ledger. Adding this letter requires first applying it as a transaction. Also, the verification task depends mainly on finding a matching hash value for the official letter that requires verification. Both services start with creating a transaction; the transaction of issuing a letter includes the letter itself, while the transaction of verification includes a hash value.

Algorithm. 1, creates a list of hash values of all the arrived transactions, and these transactions are added to an array of structure of type issue_transaction.

structure issue_transaction
{ letter: string;
client_email: string;
issuing_date: date;
issuing_time: time; }

Email, issuing_date, and issuing_time are included in the data part of the block when adding to the ledger. Only the letter field is used to create a hash value to help verify the letter as shown in Algorithm 1.

Algorithm. 1: Creating a Hash-List

```
Input: array of issue_transaction, n = no. of
issue_transaction
Output: list of hash value of letter
Begin
1: hash_list = empty
2: For count:1 to n
3:    hash-value = SHA256 (issue_transaction.
letter[count])
4:    Add (hash_list, hash-value)
5: end for
6: Return (hash_list)
End
```

The verification task depends mainly on searching the created Merkle Tree to check for the existence of an official letter. The node in the Merkle Tree is a structure of five values.

Merkle Tree node
{ hash_value string of 256 length of digits
date: date
time: time
left. node: pointer to next left node or Null
right. node: pointer to next left node or Null}

The following algorithms present the steps for implementing the Merkle Tree when one letter or a list of letters are added to the framework.

Algorithm 2: Creating the Merkle Tree

```
Input: hash_list; length=no. of transactions in
(hash_list). Merkle_Tree: Merkle Tree node
Output: Updated Merkle-Tree
Begin
1: root= Merkle_Tree1
2: For L=0 to length
3:   If (root is empty)
4:     root =hash_list[0]
5:   else
6:   {While (!(root.left ==NULL &&
root.right==NULL))
7:     if (root.left == NULL)
8:       { root.left = hash_value[l];
9:       break}
10:  else
11:        {If (root.left != NULL)
12:        root= root.left}
13:     else
14:       {if (root.right == NULL) {
15:         root.right = hash_value[l]
16:         break}
17:     else
18:       root=root.right
19:   end if
20:  end while}
21:  end if
22: end for
23: Merkle_Tree = root
24: Return (Merkle_Tree)
End
```

Algorithm 3 shows the process of verifying the existence and veracity of a document. The final result is either finding a matching hash that the document is verified or not finding a match.

Algorithm 3: Document Verification

```
Input: Document, Merkle_Tree
Output: Found as Boolean value
Begin
1: hash_doc = SHA256(Document)
2: found=false
3: While (root != Null && flag == false)
4:   If hash_doc == root. hash_value
5:     {found = true
6:      Break}
7:    else
8:     root = root.left
9:  end if
10: end while
11.While (root != Null && flag == false)
12:  If hash_doc == root. hash_value
13:      {found = true
14:       Break}
15:  else
16:   root = root.right
17:  end if
18: end while
19: return (found)
End
```

Blockchain Information and Testing Data in FBCOLM

The implementation and testing of blockchain-based applications requires deciding on the types of information fields within the block. In FBCOLM, the block is implemented as a structure that consists of the following fields of information:

- Time stamp: The date and time when the block was added to the ledger.
- Endorser: The endorsement information.
- Data hash value: Hash value of the data (using the SHA-256 hash function algorithm).
- Parent block Hash value: Hash value (head) of the previous block (using the SHA-256 hash function algorithm).
- Block hash value (head of the block): Hash value (head) of the previous block (using the SHA-256 hash function algorithm).
- Data: Text of the form shown in Fig. 4.

The system has been tested using a collection of English language official letters collected from the Internet [25]. The collected letters about 10 letters are of the form shown in Fig. 4. Each of these letters has a size up to 100 KB, which represents the data part of the blocks. These letters are used to test the work of the Merkle tree implementation and the process of a letter verification. Then a code program to generate random text that helps to measure the bandwidth of

the framework was implemented as shown in Algorithm 4.

[Name / organization Name]
[Title (Optional)]
[Address]
[Tel]
[E-mail (Optional)]
[Date]

[Recipient's Name]
[Title (Optional)]
[organization Name]
[Street Address]
[Town, County Postal Code]

Subject /

[1st paragraph of the Body of the letter]
[2nd paragraph of the Body of the letter]
[3rd paragraph of the Body of the letter]

Figure 4. The general form of the data field in the block in FBCOLM.

Algorithm 4. Generating random text for testing
Input char alphanum[] ="0123456789""!@#$%^&*""ABCDEFGHIJKLMNOPQRSTUVWXYZ" "abcdefghijklmnopqrstuvwxyz" int maxsize Output char generated_text[maxsize]
Begin 1: length = rand() % maxsize; 2: for i: 0 to length 3: generated_text[i] = alphanum[random_int mod size_of (alphanum)] 4: end for End

Results and Discussion:

The practical part of the proposed blockchain administration services has been implemented using TCP Socket programming using Java language to provide official letter archiving and management. The system has been tested using the dataset mentioned in the block information in the FBCOLM section.

The processes for verification and receipt of new documents were tested. In Fig. 5, the simulation program was tested using up to 1,000 client requests for verifications, starting from 50, 100, 200, …, 1,000 and the time in milliseconds required to process the requests, including one of the official letters in the collected dataset. The time required to complete verifications steadily increases as the number of requested verifications increases because each verification in the blockchain takes time to search for the matched hash value and requires the consent of all blockchain members in order to return the correct feedback to the clients. The time complexity of searching in Merkle tree is O(n), where n is the number of nodes in the tree. Therefore, the time for verification will increase linearly as the size of Merkle tree increases.

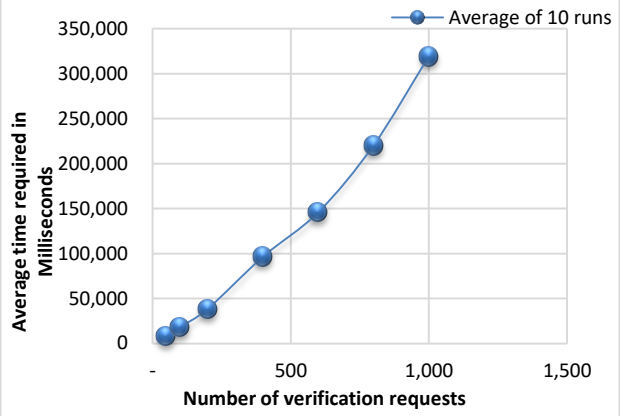

Figure 5. The average response time of 10 runs for numbers of verification requests ranges from 100 to 1,000 requests in FBCOLM.

According to the results shown in Fig. 5, the throughput of FBCOLM is 25 transactions per second. The comparison of the result of FBCOLM with some popular blockchain-based applications in Table 1 shows that the throughput of FBCOLM is accepted. The comparison result is shown in Fig. 6.

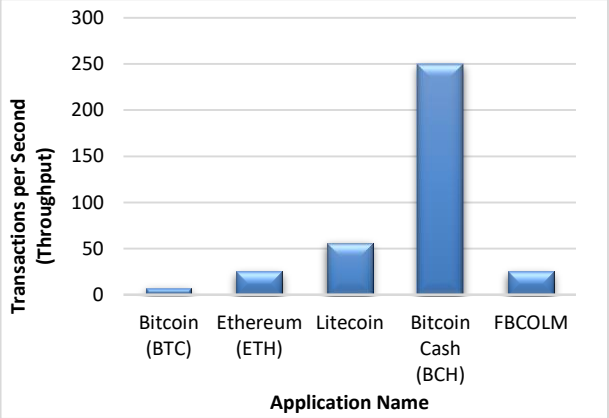

Figure 6. The competition of blockchain-based applications according to number of transactions per second

Moreover, Fig. 7, shows the client portal system's elapsed time to retrieve the number of requested documents from 100 to 1,000 documents. Elapsed time is the amount of time between the start and end of an event. This test uses Algorithm 4 in addition to time- and date-generating functions to generate a number of transactions to test the response of FBCOLM's portal. The result shows that the portal response time increases by about three seconds when the number of transaction increases from 100 to 1,000.

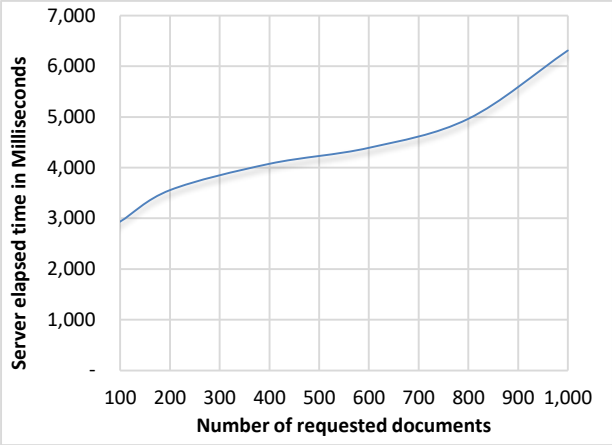

Figure 7. Client portal system elapsed time required for the different number of requests to retrieve documents.

The above-mentioned experiments and results prove that FBCOLM is characterized by following:

- High throughput: The system can process up to 200 transactions in 50 seconds, which means high throughput because there is no third party that the throughput of the system is depends on. All the services are accomplished in multiple nodes and in a distributed way.
- Scalability: The system is scalable that new nodes may be added to participate in the peer-to peer network.
- Transparency: The work is distributed to multiple nodes and none of these nodes can do the whole work alone.

FBCOLM was implemented on a network consisting of one instance of nodes for each role. This means only one portal node, orderer node, endorser node, and committer node were considered. Blockchain systems allow for an unlimited number of nodes. The challenge is to make them all participate in a distributed ledger.

Conclusion:

Building an e-government framework has typically been a difficult task because it necessitates the sharing of sensitive and private information; however, blockchain technology aids in the development of e-government systems that promote government openness while also increasing citizen interactivity. To offer verified and controlled official letter sharing, this article suggests implementing blockchain technology to issue official letters and verify them in administrative departments operations in e-government environments.

The suggested framework, FBCOLM, has been tested with various transactions to determine the time required to respond to queries. The results show that the throughput of FBCOLM is within the average range of some famous blockchain-based applications mentioned in Table. 1. Furthermore, the portal response time was tested under various densities of requests. The response delay was less than seven seconds when about 1,000 requests arrived simultaneously.

Furthermore, the proposed system was tested when there were multiple nodes participating, each one with a different role and sharing the workload of providing services.

Finally, as a suggestion for future work, adding multiple nodes for each role and testing the blockchain-based e-government services may be considered. Also, increasing the services provided by the system will be implemented as future work on the FBCOLM.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Technology.

Authors' contributions statement:

R. F. G.: created the idea of the research and manuscript, planned methodology to reach the conclusion, supervised the article and wrote result analysis and conclusions of the manuscript. A. A. S. Al.: was responsible of simulation, execution of the experiments, logical interpretation and presentation of the results. Sh. M. M.: wrote the theoretical background part of the manuscript and reviewed the article before submission.

References:

1. Afifie NA, Khang AWY, BinJaafar AS, Amin AF, Alsayaydehahmad JA, Indra WA, Herawan, SG, Ramli AB. Evaluation Method of Mesh Protocol over ESP32 and ESP8266. Baghdad Sci J. 2021; 18(4):1397-1405. https://doi.org/10.21123/bsj.2021.18.4(Suppl.).1397.
2. Hassan SF, Ghani RF. PWRR algorithm for video streaming process using fog computing. Baghdad Sci J. 2019; 16(3): 667-676. https://doi.org/10.21123/bsj.2019.16.3.0667.
3. Stuart H, Stornetta WS. How to Timestamp a Digital Document. J Cryptol. 1991; 3(2): 99–111.
4. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Decentralized Business Review. 2008; 23(4): 1-9. https://bitcoin.org/bitcoin.pdf.
5. Buterin V A. Next Generation Smart Contract & Decentralized Application Platform. Etherum White Paper. 2014; (1):1-36.

https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
6. Alshehri M, Drew SJ. E-government principles: implementation, advantages and challenges. Int J Electron Bus. 2011; 9(3): 255–270: https://doi.org/10.1504/IJEB.2011.042545 .
7. Zulkarnain PD. The E-government development towards anti-corruption strategy in Indonesia. Ph.D. dissertation, Graduate School of Asia Pacific Studies, Waseda University, Indonesia. 2017: 1-235.
8. Danielsen F, Flak LS, Ronzhyn A. Cloud Computing in eGovernment: Benefits and Challenges. ICDS 2019 : 13th Int Conf Digit Soc EGovet. 2019; 2: 71-77 http://personales.upv.es/thinkmind/ICDS/ICDS_2019/icds_2019_4_20_18002.html.
9. Naiknavare OS, Patil MP, Chawate RC, Borana AB, Sonawane S. Blockchain based Transparent and Genuine Charity Application. Int J Res Appl Sci Eng Tech. 2022; 10(3): 1909–1915. https://doi.org/10.22214/ijraset.2022.41021.
10. Cai Y, Zhu D. Fraud detections for online businesses: a perspective from blockchain technology. Financ Innov. 2016; 2(1): https://doi.org/10.1186/s40854-016-0039-4.
11. Hou H. The application of blockchain technology in E-government in China. ICCCN 2017: IEEE 2017 26th Int Conf Comp Commun Netw. July 31 - August 3. 2017; Vancouver, Canada: https://doi.org/10.1109/ICCCN.2017.8038519.
12. Liu L, Piao C, Jiang X, Zheng L. Research on Governmental Data Sharing Based on Local Differential Privacy Approach. Proc IEEE 15th Int Conf e-Biz Eng. 2018. https://doi.org/10.1109/ICEBE.2018.00017.
13. Ghani RF, Salman AA, Khudhair AB, Aljobouri L. Blockchain-based student certificate management and system sharing using hyperledger fabric platform. Period Eng Nat Sci. 2022. 10(2): 207-218. DOI: 10.21533/pen.v10i2.2839.
14. Zarrin J, Wen PhanH, Babu Saheer L, Zarrin B. Blockchain for decentralization of internet: prospects, trends, and challenges. Clust Comp. 2021; 24(4). https://doi.org/10.1007/s10586-021-03301-8.
15. Riva GM. What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights. Front blockchain. 2020; (3). https://doi.org/10.3389/fbloc.2020.00036.
16. Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proc IEEE 6th Int Cong Big Data, 2017. https://doi.org/10.1109/BigDataCongress.2017.85.
17. Zajac P. Ephemeral keys authenticated with Merkle trees and their use in IoT applications. Sensors. 2017; 21(6): https://doi.org/10.3390/s21062036.
18. Bruschi F, Rana V, Pagani A, Sciuto D. Tunneling T 103758 rust into the Blockchain: A Merkle Based Proof System for Structured Documents. IEEE Access. 2021; (9): 103758- 103771. https://doi.org/10.1109/ACCESS.2020.3028498.
19. Guo Zhan, He X, Zou Pyan. Voting system based on blockchain. J Comp Sci Res. 2021; 3(2): 27-38. https://doi.org/10.30564/jcsr.v3i2.2797
20. Nguyen GT, Kim K. A survey about consensus algorithms used in Blockchain. J Inf Process Syst. 2018; 14(1): 101-128. https://doi.org/10.3745/JIPS.01.0024.
21. Chaudhry N, Yousaf MM. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. 12th Int Conf Open Source Syst Techs 2018: 54-63. http://doi:10.1109/ICOSST.2018.8632190.
22. Kiyeng D, Karume SM, Masese N. Design of Blockchain Based Smart Contract for Tendering. Int J Comp Apps Tech Res. 2021; 10(10): 222-225. https://doi.org/10.7753/ijcatr1010.1002.
23. Khayyat M, Alhemdi F, Alnunu R. The Challenges and Benefits of Blockchain in E-government. Int J Comp Sci Net Sec. 2020; 20(4):15-20. http://paper.ijcsns.org/07_book/202004/20200403.pdf
24. Liam K. How Many Transactions Per Second—Bitcoin? [Online]. 2022; (6): Available: https://Coinformant.Com.Au/How-Many-Transactions-per-Second-Bitcoin/.
25. 9+ Official Letter Writing Examples—PDF., [Online]. 2022. Available: https://www.Examples.Com/Business/Official-Letter-Writing.Html

Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: Suppl. November 2022 **2022, 19(6): 1592-1602** **E-ISSN: 2411-7986**

إطارعمل مقترح لمشاركة الرسائل الرسمية والتحقق منها في بيئة الحكومة الإلكترونية بناءً على تقنية سلسلة الكتل

رنا فريد غني[1] **آسيا علي سلمان الكرخي [1]** **شاكر محمود مهدي [2]**

[1] قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.
[2] قسم الدراسات العليا، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة:

يساعد التقدم في شبكات الحاسوب وظهور تقنيات جديدة في هذا المجال على اكتشاف بروتوكولات وأطر جديدة توفر خدمات جديدة قائمة على شبكة الحاسوب. تم انشاء خدمات الحكومة الإلكترونية وهي نسخة حديثة من الحكومة التقليدية ، من خلال التطور المطرد للتكنولوجيا بالإضافة إلى حاجة المجتمع المتزايدة للعديد من الخدمات. ترتبط الخدمات الحكومية ارتباطًا وثيقًا بحياة المواطنين اليومية ؛ لذلك من المهم تطوير هذه الخدمات بما يتناسب مع التطورات التكنولوجية. من الضروري الانتقال من الأساليب التقليدية لإدارة العمل الحكومي إلى الأساليب التقنية المتطورة التي تعمل على تحسين فعالية الأنظمة الحكومية لتقديم الخدمات للمواطنين. تعد تقنية سلسلة الكتل من بين التقنيات الحديثة المناسبة للغاية لتطوير خدمات الحوكمة الرقمية ، وتعد قدرتها التكنولوجية على الحفاظ على استقرار المعلومات أمرًا حيويًا في أنظمة الحوكمة الرقمية نظرًا لأنها تعمل على تحسين إجراءات النزاهة والشفافية مع منع الفساد. في هذه الدراسة ، تم بناء بروتوكولات لشبكات الحاسوب لتشكل إطار عمل لشبكة تعتمد مبدأ نظير لنظيرتهدف لإدارة الوثائق الرسمية باستخدام تقنية سلسلة الكتل لتوضيح كيف يمكن تطوير أي عنصر من عناصر العمل الحكومي باستخدامها. يتضمن الإطار المقترح إضافة وثيقة رسمية جديدة ، والتحقق من وثيقة موجودة. تم إنشاء النظام بإستخدام لغة جافا واختبار أوقات الاستجابة للعديد من الطلبات المتزامنة. تم اختبار النظام باستخدام المعاملات المنجزة في الثانية. وأظهرت النتيجة أن النظام المقترح عالج 200 معاملة تحقق من المستندات في غضون 50 ثانية. بالإضافة إلى ذلك ، قدم اختبار النظام المقترح الوقت المطلوب لاسترجاع المستندات - حوالي ثلاث ثوانٍ للإجابة على 100 معاملة استرجاع وثيقة. علاوة على ذلك ، تمت مقارنة نتائج المعاملة في الثانية بنتائج نفس القياس لبعض التطبيقات الشائعة مثل البيتكوين. وكانت نتيجة النظام المقترح ضمن القيمة المتوسطة لنفس القياس للتطبيقات الأخرى التي تمت مقارنتها.

الكلمات المفتاحية: تقنية سلسلة الكتل، شبكات الحاسوب، الانظمة الموزعة، الحكومة الإلكترونية، شبكات نظير لنظير.