Engineering and Technology Journal
Journal homepage: https://etj.uotechnology.edu.iq

Blockchain-based E-Government system using WebSocket protocol

Zainab A. Kamal, Rana F. Ghani*, Alaa K. Farhan

Computer Science Dept., University of Technology- Iraq, Alsina'a street, 10066 Baghdad, Iraq.
*Corresponding author Email: rana.f.ghani@uotechnology.edu.iq

HIGHLIGHTS

- Integratating Blockchain technology and WebSocket protocol for public service Delivery.
- Blockchain's security and WebSocket's connectivity enable real-time, efficient communication with under 3s latency.
- Providing Real-time connectivety and connectivety enhancement.

ARTICLE INFO

Handling editor: Mohammed Y. Hassan

Keywords:
E-government
Blockchain
WebSocket Protocol
MongoDB
Performance

ABSTRACT

This paper explores integrating Blockchain technology and WebSocket protocol to implement an E-government system. Blockchain is used to record correspondence between users and the government, while WebSocket is used to communicate among the distributed nodes of the blockchain network. This system leverages the inherent security and transparency of blockchain in addition to the real-time communication capabilities of WebSocket, which elevate the performance of the delivered services by the government. In this paper, users can submit transactions and track them in a way that allows them to follow up on all actions taken regarding their transactions. Information and framework transactions are stored in the MongoDB system and retrieved when needed. Also, previous transactions can be verified using the Merkle tree. This paper highlights the potential benefits of the proposed system. The system has been tested considering various factors related to end-user perception, such as transaction request, latency, and throughput. Furthermore, practical use cases are discussed to adopt the proposed system successfully. The proposed system ensures the active participation of all the nodes in the system without making an individual decision in favor of a particular node or the citizen's interest.

1. Introduction

In our contemporary life and present, it is difficult to coexist without computer networks, as their role is great in ordinary, practical, and economic life. The necessity of computer networks brought about vast development, as they facilitated communication, and it became easy to transfer information quickly. This immensely benefited several areas, including education, medicine, and industry. Because of the rapid development of computer networks, there was a need to use them in governments, which led to a noticeable change in the completion of transactions and the provision of public services. Initially, the reliance on centralization was on a central authority, but recently, governments began to move towards decentralization and rely on blockchain (BC) networks [1,2].

Blockchains provide the opportunity to organize the exchange and retrieval of information between many government agencies. Blockchain Technology applications can effectively provide government services by breaking down the central information and the shift towards decentralization between these organizations and governments [3,4]. Blockchains provide data sharing and confidentiality, allowing people to create new programmable frameworks. Blockchains lead to improvement and the establishment of connected service centers and organizations, as they support clear, modified, and well-organized procedures for communication [5].

Researchers have recently highlighted the potential of BC technology and distributed ledger technology to revolutionize government operations [6]. BC-based applications have the advantage of improving the efficiency of information exchange and providing high performance in distributed and decentralized environments [7]. Blockchains provide great benefits and potential, as they are a technology that builds a trustworthy service in an untrustworthy environment [8].

Blockchain is a distributed and peer-to-peer system with no third-party node or main node within blockchain systems. One of the blockchain platforms may be used to implement a BC-based application, such as Ethereum or Hyperledger, or it may be implemented using a programming language with other software tools. This work aims to implement blockchain technology from scratch using C# programming language and deploying this application using web Socket.

http://doi.org/10.30684/etj.2024.146559.1689
Received 03 February 2024; Received in revised form 29 March 2024; Accepted 01 April 2024; Available online 14 April 2024
2412-0758/University of Technology-Iraq, Baghdad, Iraq

WebSocket is a communication protocol that provides bi-directional communication between servers and clients. This two-way communication capability makes WebSocket ideal for implementing collaborative tools and functions within distributed applications [9].

In this paper, a blockchain technology framework has been implemented using Web Socket. This framework has been used to implement the services of an e-government system.

The article is structured as follows: The related work that has been highlighted is appropriately presented in section 2. Section 3 describes the architecture of Blockchain Technology. Section 4 describes the web socket; Section 5 shows the measurements used to test the proposed system. The proposed e-government system is presented in section 6. 7 presents the results of testing the proposed system. The last section is the conclusion..

2. Related work

Various papers suggested frameworks for e-government systems using blockchain technology. In this section, we have reviewed some of these papers to compare their framework with the one proposed in this paper.

Elisa et al. [10] proposed a framework for an e-government system. The framework depends on BC to increase public sector trust by improving information security and privacy. A prototype of the proposed system was presented in this paper. The system can ensure the confidentiality, integrity, and availability of services and protect against cyber-attacks such as attempts to alter and/or unauthorized access. Assiri et al. [11] proposed an e-Government framework that leverages blockchain technology to improve security and privacy issues in the Saudi e-Government system. The proposed framework integrates blockchain technology into e-Government to increase cyber-attack resistance for the system and users. The blockchain technology brings decentralization, access control, confidentiality, privacy, and trust into the e-Government service. The framework also includes an intrusion prevention system (IPS) and a router firewall to detect and prevent internal and external attacks. Meirobie et al. [12] presented a document verification method based on BC, allowing for faster block insertion into the chain. Ghani et al. [13] presented an architecture that utilizes the capabilities of blockchain technology to issue and verify student certifications in a verifiable and efficient manner. The proposed e-certificate framework provides controlled data sharing through a smart contract. To provide privacy for students' information, the students' records are stored in a local database, while the blockchain only contains e-certification data. However, access to private information is possible with the approval of the blockchain-authorized user. Ghani et al. [14] proposed a framework that provides a secure and efficient solution for official document management in an e-government environment. The framework is designed to improve document management's efficiency, security, and transparency in public and private sector institutions.

The proposed work could offer several benefits, some shared with related work while others distinctive. Using blockchain technology provides transparency and accountability in the e-government system by providing an immutable and transparent ledger of transactions. Also, BC enhanced the security and privacy of sensitive government data. Besides transparency and security, BC technology increases the efficiency of service delivery to the end user and reduces the reliance on centralized authority. Finally, using the WebSocket protocol to implement a Blockchain-based e-government system has enabled real-time communication between users and e-government.

3. Blockchain technology for e-government systems

BC technology was first used by Satoshi Nakamoto in 2008. Then, they improved the design by adding a hash to timestamp blocks without the need to sign documents. A BC is a list of records, called blocks, that are linked together using a hash function. Each block contains a hash value of the previous block, a timestamp, and transaction-specific data [15-17]. BCs are managed by peer-to-peer (P2P) networks, nodes working collectively to communicate and validate new blocks. Therefore, blockchain is considered a distributed computing system technique with a high fault tolerance [18-23].

Blockchain technology has various characteristics that make it appropriate for implementing and managing the services of e-government systems. The following are the key blockchain technology characteristics for e-government systems:

1) Immutability means that records committed to the BC never change. This property enhances transparency and makes the system resistant to corruption [19].
2) Decentralization means there is no third party to govern and control e-government services. A group of nodes maintains the network, which makes it decentralized [20].
3) Enhancing security: Since the BC eliminates the central authority, no one can change any network properties to their advantage. Using hash value guarantees another layer of security for the system [21].
4) Distributed ledger: The ledger will provide all the information about the transaction and the participants. People can see what is happening in the ledger, and because it is in the network, it is maintained by all other users on the system [22].
5) Consensus: The core of BC systems is consensus algorithms. A consensus algorithm is the blockchain process that achieves agreement on a single transaction among nodes [24-25]. There are various consensus algorithms: proof of work (POW) [26], practical Byzantine fault tolerance (PBFT) [27], and proof of stack (POS) [28-29].

4. WebSocket protocol background

Web Socket is a two-way communication protocol based on the Transmission Control Protocol (TCP) that unifies the communication between the client and the server. Both parties are allowed to request data from each other. This protocol is

suitable for web-based near real-time traffic required in games, chats, stock exchange information systems, multimedia systems, remotely controlled systems, etc. [30]

The web connection between the client and the server can remain open if the parties wish to maintain the connection, allowing continuous communication. There are two ways for the server to send data to the client. The client can regularly request data from the server, known as polling, or the server can automatically send data to the client, known as server pushing [31].

Figure 1 shows a sequence diagram of a WebSocket session and emphasizes the communication overhead the WebSocket protocol requires [9].

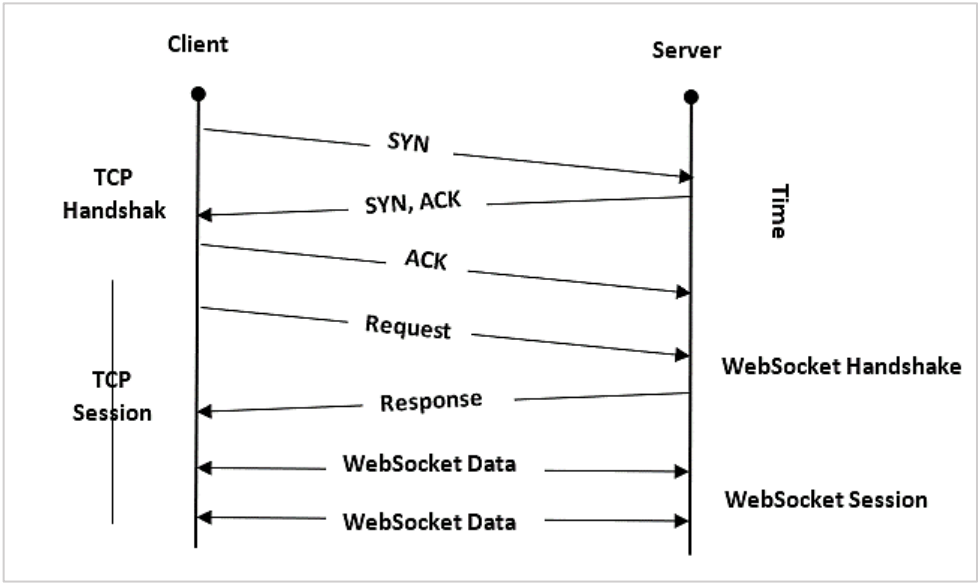

Figure 1: WebSocket Protocol Sequence Diagram

5. Blockchain performance measurements

Blockchain performance is measured by the following measurements:

5.1 Flow of data in the BC

Traditionally, the flow of data is thought of as a continuous flow, but the rate of data flow varies; it is periodic, not continuous, and the periodic flow is the update rate.

5.2 Transaction latency

The time scale by which a transaction is sent to the network until the time a transaction is written in the ledger. This metric is measured by checking the timestamp of transactions and comparing the time they were sent to when they are validated or stored according to Equation 1. This scale provides insight into how quickly the adopted algorithms and mechanisms are implemented [32].

$$Transaction - Latency = Confirmation_{time} - Submission_{time} \quad (1)$$

5.3 Speed

The network's average latency rate (block and transaction time).

5.4 Network response time

The community is accustomed to instant communication, which means the transmission of transactions over the network, and the time required to create blocks containing transactions is the time required for the transaction to appear on the BC [33].

5.5 Transaction throughput

The valid transaction rate is complete and recorded in blocks. As in Equation 2, it is the number of transactions that have been committed and validated, and this does not represent the transfer of transactions in one node but in all nodes [34, 35].

$$Transaction - Throughput = \frac{No.of\ Commited\ Transactions}{Total\ Time} \quad (2)$$

Total time is measured in seconds.

6. The proposed E-Government system based on blockchain and WebSocket protocol

In this paper, digital government transactions have been implemented using BC and exchanged using web-socket to represent a framework for e-government systems. Blockchain technology is the most efficient technology for sharing data in a controlled way without losing ownership and storage across P2P systems in distributed and untrusted networks. The proposed system is implemented as a distributed ledger supported by smart contracts. It consists of two layers: the external layer which represents the citizen account and the Internal layer, which represents the blockchain and refers to a group of nodes responsible for verifying and authenticating transactions. Nodes collectively process transactions and are either accepted or rejected. The proposed system includes the following parts:

6.1 Distributed ledger

A sequential, tamper-resistant ledger. It results in a set of blocks, and each block contains several transactions. Each peer keeps a copy of the ledger. The transactions are encrypted before adding to the ledger to provide privacy and security for the users.

6.2 Nodes

The system consists of a network of nodes, each of the participant nodes has its role:

- Orderer Node: This is the counterpart that distributes transactions to legal nodes.
- Legal Node: This peer belongs to the network and performs several roles, such as recording data and verifying transactions.
- Commit Node: This is the node that receives a set of transactions that have been created and verified. The node records it in the ledger.
- Anchor Node: This is a peer that communicates with others in another organization.

6.3 Consensus

The system provides a consensus mechanism to validate the transactions. The proposed system depends on the Byzantine consensus algorithm.

Any processing or correspondence between the citizen and the nodes would be recorded in BC. High security will be followed to prevent intruders from unauthenticated access to the system. Dealing with unstructured rules is done by using MongoDB, which includes the data and links it to a web page to allow the client node to verify for themselves the decision that the government will take. Figure 2 shows a business model for creating an E-governance based on the BC.

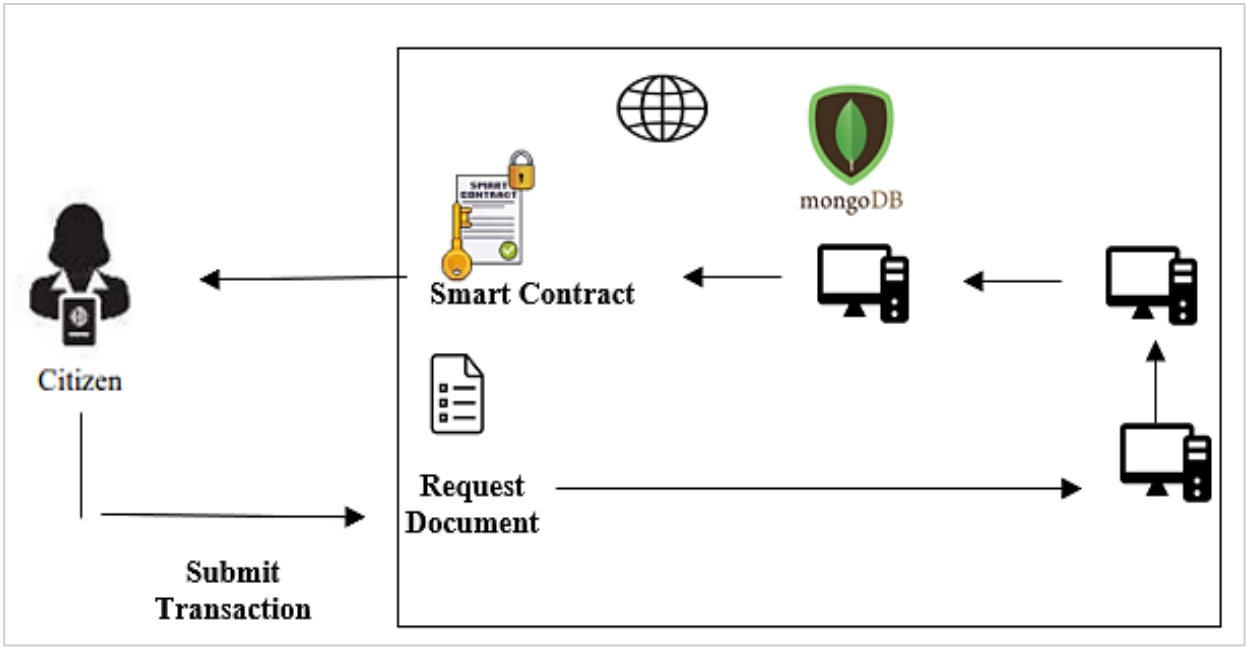

Figure 2: Sequence Diagram for Creating an E-Governance Based on the Blockchain

The data is organized depending on its hash value. Each transaction has its hash generated from the data. The block of transaction data is used to build a Merkle tree. The system also uses MongoDB to store the original data. After the data is built in a Merkle tree, depending on hash functions, it will be verified by the hash within the Merkle tree. Figure 3 shows a sequence diagram for creating the proposed BC-based E-governance framework.

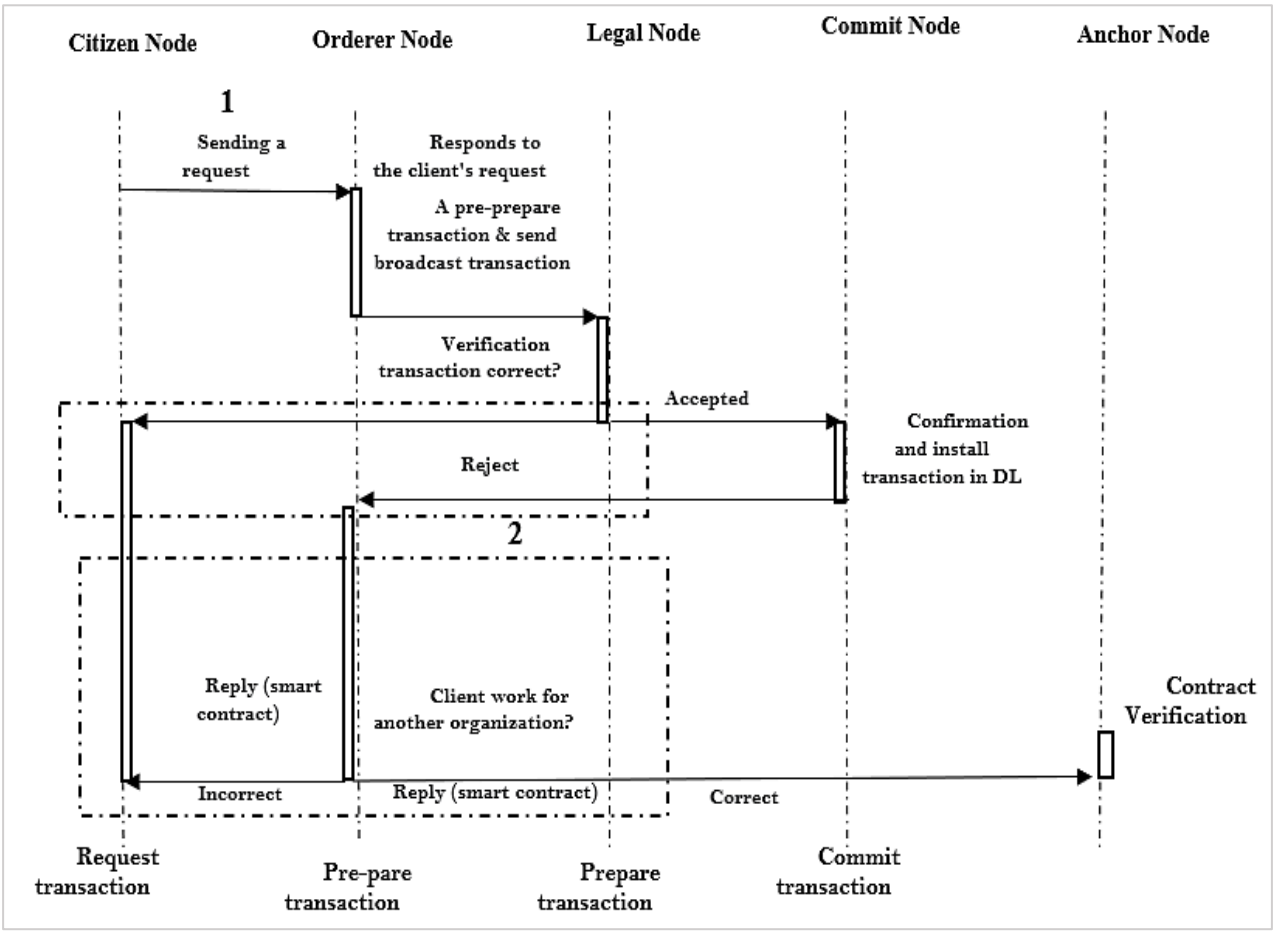

Figure 3: A Business Model for E-Governance Based on the BC

7. Results and discussion

The proposed E-government system implemented using BC technology and Web Socket has been tested according to the metrics explained in section 5. The results are shown in this section. The system that has been tested considers the factors related to end-user perception, such as transaction request, latency, and throughput. Initially, the time taken to receive a transaction from a citizen was tested, and it was 300 ms. The user transactions are verified in a very short time. Increasing the number of validators in the network will reduce the time required to process the transactions. Therefore, a sufficient number of validators provides better verification of transactions. A network of validators can validate many transactions in less than a second. Figure 4 shows the performance of the proposed system according to the increase in the number of validators in the system. As expected, decreasing the number of validators increases the throughput of the proposed system. However, increasing the validator increases the validation of a transaction. Therefore, it is essential to compromise between increasing the number of validators and the system throughput.

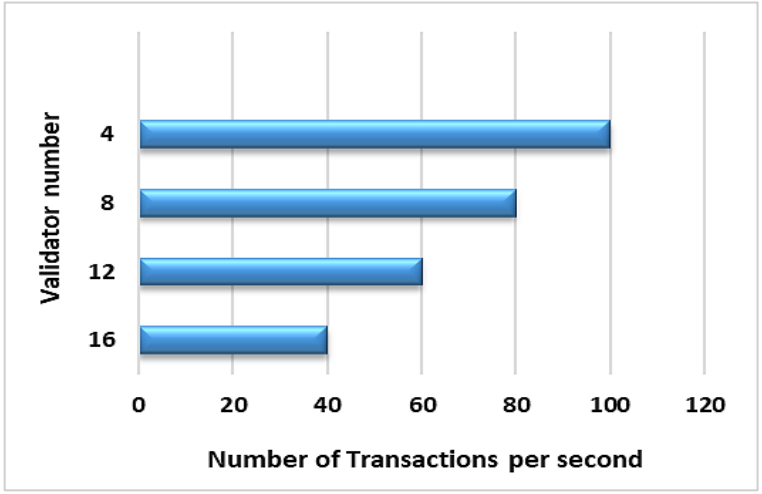

Figure 4: Transactions Per Second Against Validators number

Figure 5 shows the throughput of the proposed system in various densities of the workload circumstances. The time increases linearly with the increment of the number of concurrent transactions.

Here, the transaction throughput has been tested. It does not represent the transfer of transactions in one node but the time required to process the transaction in all nodes. Figure 6 shows the relation between committed transactions and time.

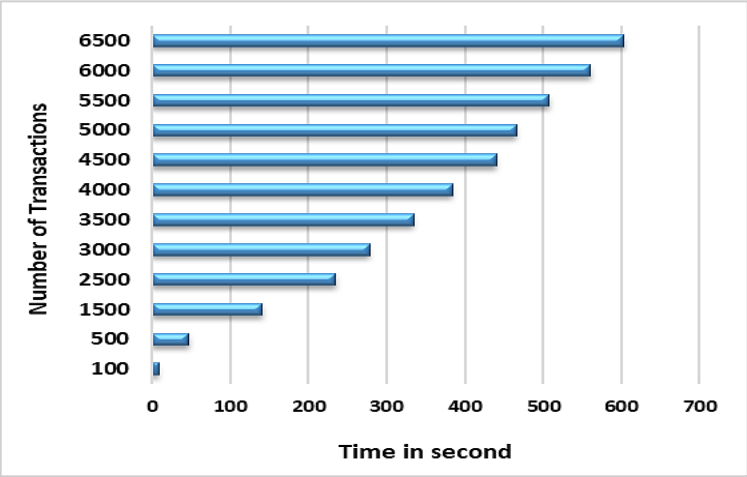

Figure 5: Transactions Throughput

Figure 6 shows the results of the Transaction Latency of the proposed system. The transaction response time is the amount of time it takes for a transaction to become usable across the network, including the consensus mechanism decision time. The average transaction latency of three transactions is 2500 milliseconds. This time results from all the processing stages applied to the transaction, from submission to the appearance of the result to the user. The factors which affect the transaction latency are: the network congestion, BC consensus mechanism, the system architecture, the transaction complexity and BC network scalability. When the transaction latency is tested some of these factors are identical such as consensus mechanism and the system architecture, while other factors such as the network congestion are variable. Therefore, the value of transaction latency is not the same for all transactions.

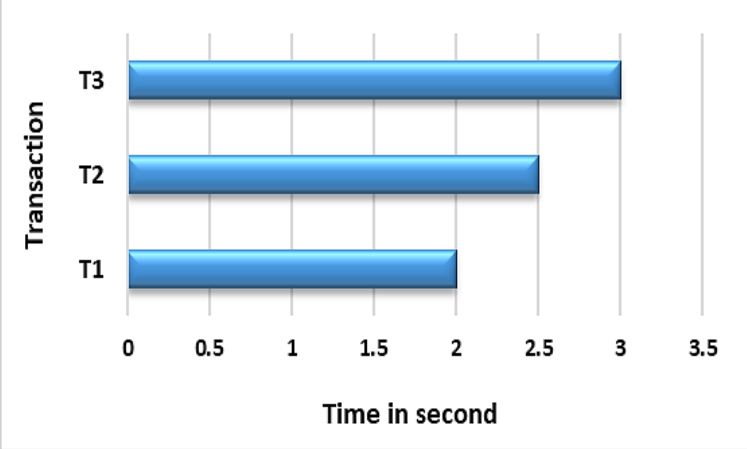

Figure 6: Transactions Latency of three transactions

Data within the proposed system is stored using MongoDB. It is accessed and retrieved depending on the hash value in MongoDB. In the ledger, the transaction is organized in blocks, and the transaction is verified using the Merkle tree, which contains the hash function of the data for each transaction. This work implements the system using MongoDB and then an SQL server. Table 1 shows the time required to retrieve data from the SQL server and MongoDB. Both of the DB systems are added to a version of the implemented proposed system to compare the retrieving time between in the context of BC based e-government system. MogoDB retrivening time is less than the time required to retrieve data from SQL server. Therefore, the final version of the proposed system uses MogoDB.

Table 1: Retrieving Data by SQL and MongoDB

Transaction	Retrieving time in SQL Server	Retrieving time in MongoDB
T1	7s	5s
T2	5s	3s
T3	7s	4s
T4	8s	5s

From Table 1, we can see MongoDB provides better retrieving time than SQL server DB because of JSON data support provided by MongoDB natively, which is aligned with BC technology, making data retrieval more efficient. Finally, the proposed framework has been compared to the reviewed frameworks in section 2. The result of the comparison is shown in Table 2. The comparison depends on four factors. The first factor is the main aim of the work. Secondly, the related works and the proposed system have been compared according to the BC type used. Thirdly, the software and platform are used to implement the work. The last factor is the evaluation measurement of work.

We can see in Table 2 that there is a similarity between the proposed system and some of the related works in each of these factors. However, the proposed system offers an improvement in using BC technology to implement e-government systems. The proposed system exploits the real-time feature of WebSocket protocol to manage and efficiently provide e-government service. Also, the proposed system has been evaluated using the transactions per second metric. Although the related works [13] and [14] had used the same metric, it could not be compared because the transaction size and the required processing are different.

Table 2: A Comparison with the reviewed frameworks

Comparison factor	**[10]**	**[11]**	**[12]**	**[13]**	**[14]**	**The proposed System**
Aim	increasing the trust of the public sector by improving information security and privacy	Securing and improving the privacy of the Saudi e-Government system.	Securing Documents in E-government systems	issue and verify student certifications in a verifiable and efficient manner	digitally transforming the work of administration departments in organizations through the use of BC.	A framework to manage the services in an e-government system securely and efficiently in real time.
BC Type	private	either public or private	Private	Private	Private	Hybrid
Software and platforms	Unknown	Unknown	The software used to implement this work includes HTTP servers, Python 3, and the Flask framework.	Hyperleadger	Java Language	C# and WebSocket Protocol
Evaluated	Security key length	various penetration testing tools	Unknown	Transaction per Second	Transaction per Second	Transaction per Second

8. Conclusion

In conclusion, this paper has introduced a novel approach to implementing an e-government system using Blockchain technology and WebSocket protocol. The research results and experiments demonstrate the feasibility of using these technologies together to implement an e-government system efficiently. The proposed system leverages temper-proof and decentralization of blockchain technology while exploiting the real-time communication ability of WebSocket protocol. The latency time is tested, and the average is less than 3s. The use of a Merkle tree was based on the hash of all the data to search and obtain data and ensure that the data has not been subjected to any manipulation quickly and effectively. Moving forward with this research may focus on scalability and addressing more privacy and security concerns.

MongoDB provides efficient retrieving time because of JSON data support provided by MongoDB natively, which is aligned with BC technology, making data retrieval time more efficient.

Author contributions

Conceptualization, R. Ghani, Z. Kamal. and A. Farhan; data curation, Z. Kamal.; formal analysis, R. Ghani, Z. Kamal. and A. Farhan.; investigation, Z. Kamal.; methodology, R. Ghani, and Z. Kamal.; resources, Z. Kamal.; software, Z. Kamal.; supervision, R. Ghani.; validation, R. Ghani, Z. Kamal. and A. Farhan.; visualization, R. Ghani and A. Farhan.; writing—original draft preparation, Z. Kamal.; writing—review and editing, R. Ghani. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of interest

The authors declare that there is no conflict of interest.

References

[1] A. Zwitter and J. Hazenberg, Decentralized network governance: Blockchain technology and the future of regulation, Electron. J., 2020. 3 (2020). https://doi.org/10.3389/fbloc.2020.00012

[2] B. A. Forouzan, Data Communication and Network, 6th ed. Boston: McGraw-Hill, 2001

[3] R. Schollmeier, A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications, Proceedings First International Conference on Peer-to-Peer Computing, Linköping, Sweden, 2001, 101-102. https://doi.org/10.1109/P2P.2001.990434

[4] A. Ali, M. Rahouti, S. Latif, S. Kanhere, J. Singh ,Blockchain and the future of the Internet: A comprehensive review, IEEE, 2019. 1 https://doi.org/10.48550/arXiv.1904.00733

[5] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Pearson, 2010.

[6] K. Marossy, G. Csucs, B. Bakos, L. Farkas, and J. K. Nurminen, Peer-to-peer content sharing in wireless networks, in IEEE 15th Int. Symposium Personal, Indoor, and Mobile Radio Comms, 2004. https://doi.org/10.1109/PIMRC.2004.1370846

[7] M. T. Özsu and P. Valduriez, Principles of Distributed Database Systems.Book, Springer Cham, 2019. https://doi.org/10.1007/978-3-030-26253-2

[8] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, 18 (2016) 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

[9] Alex Diaconu, The WebSocket Handbook, Book, Ably, 2022.

[10] N. Elisa, L. Yang, et al. A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Netw, 29 (2023) 1005-1015. https://doi.org/10.1007/s11276-018-1883-0

[11] H. Assiri, P. Nanda, M. Mohanty, A novel e-government framework using blockchain, J. Inf. Assur. Cyber ., 2021 (2021) 1-14. https://doi.org/10.5171/2021.164568

[12] I. Meirobie, A. Irawan, H. T. Sukmana, D. P. Lazirkha, N. P. Santoso, Framework Authentication e-document using Blockchain Technology on the Government system, Int. J. Artif. Intell. Res., 6 (2022). https://doi.org/10.29099/ijair.v6i2.294

[13] R. F. Ghani, et al, Blockchain-based student certificate management and system sharing using hyperledger fabric platform. Period. eng. nat. Sci., 10 (2022), 207–218, http://dx.doi.org/10.21533/pen.v10i2.2839

[14] R. F. Ghani, et al, Proposed Framework for Official Document Sharing and Verification in E-government Environment Based on Blockchain Technology. Baghdad Sci. J., 19 (2022) 1592. https://doi.org/10.21123/bsj.2022.7513

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in IEEE Intern. Congress Big Data, (2017) 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[16] E. Zaghloul and T. Li, Bitcoin and blockchain: Security and privacy, IEEE Internet of Things J., 7 (2020). https://doi.org/10.1109/JIOT.2020.3004273

[17] A. Razzaq et al. Use of blockchain in governance: A systematic literature review, Int. J. Adv. Comput. Sci. Appl., 10 (2019). https://dx.doi.org/10.14569/IJACSA.2019.0100585

[18] N. K. Tran, Application of blockchain technology in sustainable energy systems: An overview, Sustainability, 10 (2018) 3067. https://doi.org/10.3390/su10093067

[19] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, Proc. the 17th IEEE/ACM Int. Symp. Cluster, Cloud, and Grid Computing, (2017) 468-477. https://doi.org/10.1109/CCGRID.2017.8

[20] D. Shrier, W. Wu, and A. Pentland, Blockchain & infrastructure (identity, data security), Massachusetts Institute of Technology-Connection Science, 2016.

[21] L. Lamport, R. Shostak, and M. Pease, The Byzantine generals problem, ACM Trans. Program. Lang. Syst., 4 (1982) 382-401. https://doi.org/10.1145/357172.357176

[22] Y. Yuan and F. Wang, Blockchain and cryptocurrencies: Model, techniques, and applications, IEEE Trans. Syst. Man. Cybern. Syst., 48 (2018) 1421-1428. https://doi.org/10.1109/TSMC.2018.2854904

[23] E. Zaghlouland and T. Li, Bitcoin and Blockchain: Security and Privacy, IEEE Internet Things J., 7 (2020). https://doi.org/10.1109/JIOT.2020.3004273

[24] H. Vu and H. Tewari, An efficient peer-to-peer Bitcoin protocol with probabilistic flooding, Research Gate, 285 (2019) 29-45. https://doi.org/10.1007/978-3-030-23943-5_3

[25] G. Karame, E. Androulaki, and S. Capkun, Two Bitcoins at the price of one? Double-spending attacks on fast payments in Bitcoin, IACR Cryptology ePrint Archive, 2012. https://eprint.iacr.org/2012/248,

[26] S. Almajali, Blockchain technology consensus algorithms and applications: A survey, Princess Sumaya University for Technology, Amman, Jordan, 14 (2020) 142–156. http://dx.doi.org/10.3991/ijim.v14i15.15893

[27] C. Nguyen and E. Dutkiewicz, Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications, and opportunities, IEEE Access, 7 (2019) 85727-85745. http://dx.doi.org/10.1109/ACCESS.2019.2925010

[28] M. Kouhizadeh and J. Sarkis, Blockchain practices, potentials, and perspectives in greening supply chains, Sustainability, 10 (2018) 3652. https://doi.org/10.3390/su10103652

[29] S. Makridakis and K. Christodoulou, Blockchain, Current challenges and future prospects/applications, IEEE, 11 (2019) 258. https://doi.org/10.3390/fi11120258

[30] Q. Liu, X. Sun, Research of Web Real-Time Communication Based on Web Socket, Int. J. Commun. Network & Syst. Sci., 5 (2012) 797-801. https://doi.org/10.4236/ijcns.2012.512083

[31] Wang, V. , Salim, F. , Moskovits, P. , The Definitive Guide to HTML5 WebSocket, Apress Berkeley, CA, 2013. https://doi.org/10.1007/978-1-4302-4741-8

[32] M. Catt, Blockchain fundamentals: Latency & capacity-featuring the ark ecosystem, The University of Kansas Blockchain Institute, Jul. 2018.

[33] S. Mahavir and S. Theja, Throughput optimal routing in blockchain-based payment systems, IEEE Transactions on Control of Network Systems, 8 (2021). 1859-1868. https://doi.org/10.1109/TCNS.2021.3088799

[34] M. Dabbagh and A. Beheshti, A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities, Comput. Secur., 100 (2021) 102078. https://doi.org/10.1016/j.cose.2020.102078

[35] S.S. Abdul-Jabbar, A.K. Farhan, R.F. Ghani, Data Analytics and Blockchain: A Review, Iraqi Journal Of Computers, Communications, Control And Systems Engineering, 23 (2023) 23-34. https://doi.org/10.33103/uot.ijccce.23.1.3