ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 1, February 2022, pp.620-631

E-government based on the blockchain technology, and the evaluation of its transaction through the number of transactions completed per second

Zainab Ali Kamal [1], and Rana F. Ghani [2]
[1,2]Computer Sciences Department, University of Technology-Iraq, Baghdad, Iraq

ABSTRACT

Blockchain technology is one of the basic technologies for securing data sharing and storage across peer-to-peer systems in a distributed and untrusted network. Information is stored in electronic governance, which is considered sensitive data about citizens and companies and is the focus of external attacks. E-government has one point of failure and depends on centralization, and the decision is in the hands of one party or one official. Therefore, a secure and distributed electronic system for e-governance based on blockchain technology has been proposed. The system consists of several entities, organizations or nodes responsible for consensus to make decisions. Users are given the right to raise a transaction or send a request. The transaction is evaluated by auditors, and the citizen acquires a smart contract as a way out. The proposed system was compared with electronic governance systems without the use of blockchain technology. The proposed system was tested and compared with the previous systems, and it was found that the proposed system was superior in terms of security, the speed of processing the transaction and the time of filing the transaction.

Keywords: Blockchain, DLT, E-government system and Validators.

Corresponding Author:

Rana Fareed Ghani
Department of Computer Science
University of Technology- Iraq
Baghdad- Iraq
E-mail: 110016@uotechnology.edu.iq

1. Introduction

Transactions between parties in the current systems take place in centralized form that requires the participation of a trusted third party, but which results in a single failure point and high fees of transaction. Blockchain technology addresses those issues by allowing the interaction of the untrusted entities with each other in distributed way without involving any trusted third party. Block-chain represents a data-base which records all the transactions occurring in any network. The blockchain has been proposed in Bitcoin, as it is a peer-to-peer digital system that has been developed into a scalable technology based on decentralization [1-3]. Blockchain allows untrusted participants to communicate with one another in a secure manner without needing any trusted third parties. So the blockchain can be considered as an ordered list of blocks. Every one of the blocks has been identified by cryptographic hash, and every one of the blocks refers to the block it came from, which leads to block chains. And every block consists of a series of the transactions, and as soon as a block has been created and attached to blockchain, this file cannot be changed or undone [4]. We find that the origin of the blockchain was mentioned in a paper that has been published by the name of S. Nakamoto. The network consists of a group of members who act as a contract through which correspondence takes place within the peer-to-peer network [5, 6]. Blockchain technology represents a combination of several technologies, like cryptography, algorithms, mathematics, etc.

Technology consists of six components as follows:

- **Decentralization:** Each node can be a master node that records, stores and updates the ledger.
- **Transparency:** The block data is recorded by every one of the nodes and distributed amongst the other nodes that are connected, resulting in the creation of the transparency amongst nodes.
- **Consensus:** The change is not accepted until after Consensus between the nodes and all nodes are eligible for the transfer and updating, but after unanimity. The change is not made unless a person is able to control more than 51% of the contract at the same time.
- **Anonymous:** for the purpose of making the transaction anonymous, the data is hashed prior to being shared, which is performed with the use of secure algorithms.
- **Open Source:** the majority of the block-chain systems are open source and allow participants to alter code such that it suits their needs [7, 8].

1.1. Structure of the blockchains

Every one of the blocks in a block-chain consists of 5 elements:
Main data, hash of previous block, the current block hash, other information timestamp.

- **The main data: -** which is dependent upon the transaction type in general.
- **Previous block hash:** in the case where a transaction has been executed, it has to create a hash and broadcast it to network. There are many hash algorithms that are being widely used, however, the most common one of them is Merkle tree. These algorithms allow for easy hashing or defragmentation, which is why merkel is a popular choice.
- **Current block hash:** The final value of the hash is recorded in the header of the block (the current block hash) whereas actual content is stored in block's body.
- **timestamp:** when a block was created
- **Nonce and other information such as the block signature.**

Figure 1 shows the data structure of the blockchain.

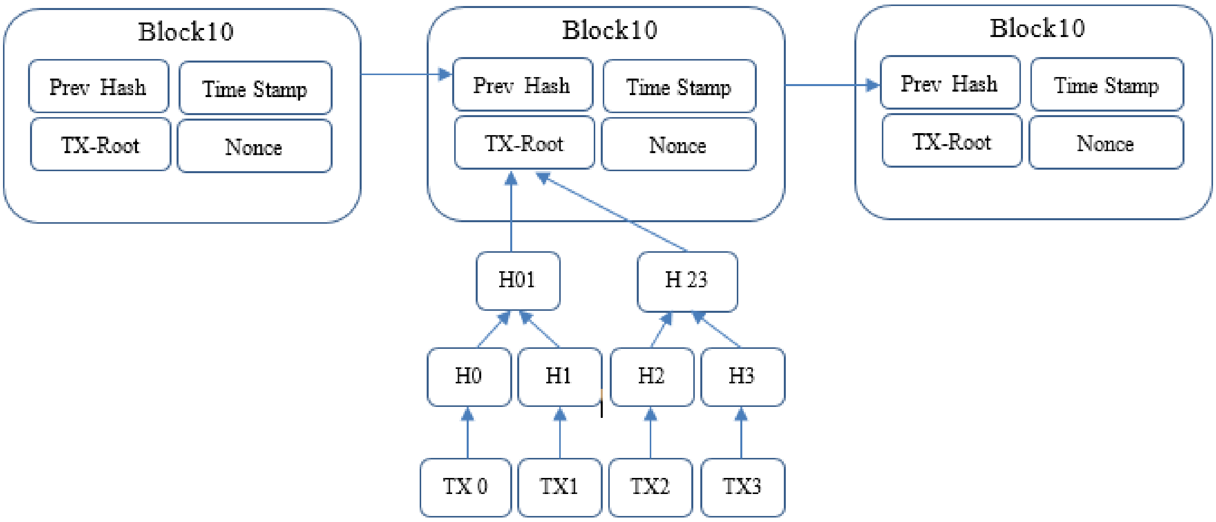


Figure 1. Bitcoin transactions' block structure [9]

A cryptographic hash function represents a review process that is performed on each block of data. The data is presented in sequential way to all of the parties on a network with appropriate access levels. The time that is needed for the verification and recording of transactions on distributed ledger technology differs according to utilized process [10-13].

2. Distributed ledger technology

The evolutions of the ledger from centralization to distribution. Block-chain provides a data-base which operates on a distributed network that is usually known as a general purpose technology or serious innovation [14].

The blockchain is under development and is considered a new mechanism to provide trust while providing a mechanism for anonymity of the contract in transactions [15, 16].

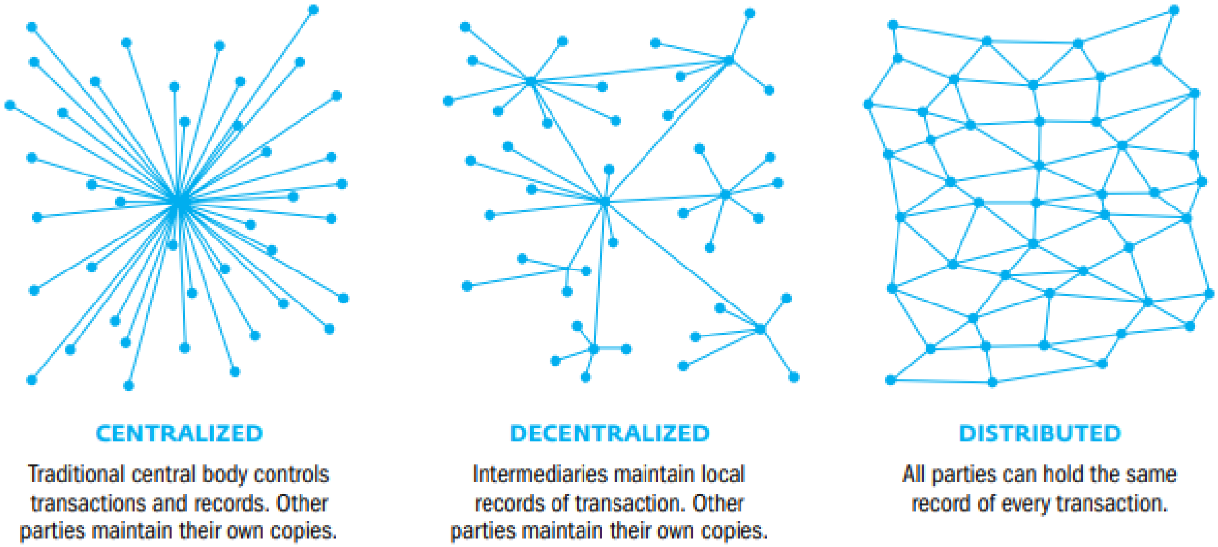

CENTRALIZED
Traditional central body controls transactions and records. Other parties maintain their own copies.
DECENTRALIZED
Intermediaries maintain local records of transaction. Other parties maintain their own copies.
DISTRIBUTED
All parties can hold the same record of every transaction.

Figure 2. Centralization, decentralization and distributed [17]

Figure 2 shows us the difference between centralization, decentralization and distribution

Centralized structure: It is one of the most famous structures in network systems, unlike decentralization. Each node is a client responsible for making its own decision, and each node is directly linked to a central server. The architecture of the central architecture is client-to-server, and by creating a common center between them, it becomes easier to send information to the system by providing a database. Thus, the database makes the system centralized and highly reliable.

Decentralization structure: is to delegate the organization's activities to planning and decision-making far from what is expected.

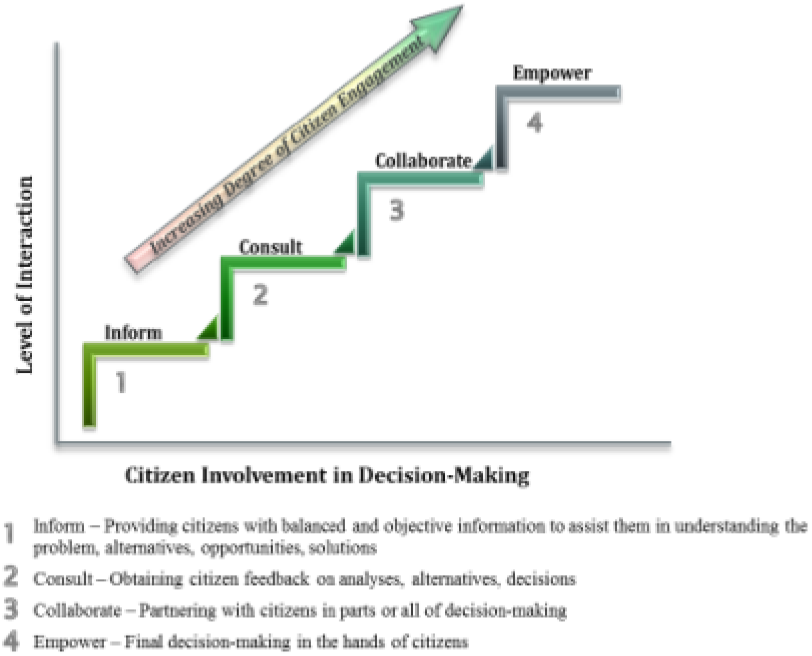
Distribution structure: They are multiple entities that have the ability to cooperate between them, and each entity has an independent opinion, and when these entities agree, they can interact, and when they do not agree, they cannot [18, 19].

2.1. Main benefits for the distributed ledger technology

- Privacy is maintained via encryption techniques.
- Distributed, sustainable, and up-to-date with every transaction, automatically shared between subscribers and in real time.
- Authentication and verification of the transaction.
- Auditability.
- Participants cannot tamper with the transaction history.
- Participants in a transaction can access same records and are allowed to identity verification.
- Consensus-based in which network participants must agree to the transaction and verification is done by consensus algorithms [20].

3. Blockchain and e- governments

E-governance is one of the concepts in public administration. The concept of e-governance recognized the roles of digitization as input or as a factor, as it focuses on the user, as these services benefit from digitization and information assets. Digital governments can be classified into three groups (government to government (G-G) - government to citizen (G-C) -government to business (G-B)). Government to government provides an online interaction between governments, authorities, and organizations to disseminate information. Government to Citizen and Government to Business allow citizens and electronic companies to ensure security and privacy in order to increase trust within the government. Citizen participation is a two-way interaction between citizens or the private sector. The citizen is given a share in decision-making in order to improve intermediate and final development, and is represented by the participation of citizens in consultation, cooperation and access to information.


Increasing Degree of Citizen Engagement
Empower
4
Collaborate
3
Consult
2
Inform
1
Level of Interaction
Citizen Involvement in Decision-Making

1 Inform – Providing citizens with balanced and objective information to assist them in understanding the problem, alternatives, opportunities, solutions

2 Consult – Obtaining citizen feedback on analyses, alternatives, decisions

3 Collaborate – Partnering with citizens in parts or all of decision-making

4 Empower – Final decision-making in the hands of citizens

Figure 3. Dimensions of citizen engagement [21]

Source: Adapted from "IAP2 Spectrum of Public Participation," International Association for Public Participations.

Among the challenges in citizen participation:

- Limited trust: in the government and it is considered the main challenge to start consultations and build trust. Government actions are often seen as low due to weak public trust and for many reasons including failure to fulfill stated promises, corruption and nepotism
- Political hesitation: essentially, the public participation represents a political process and it's usually not formalized or carried out in an organized way, and it's usually difficult to link participation to positive changes in the daily lives.
- Limited ability to participate: so as to participate profoundly in the discussions of the public policy, it's essential that the participants are aware of the issues that are at hand.
- Lack of commitment: Participation in the policy-making operations is a long-term operation that requires the people to make commitments of long-term nature.

Blockchains represent one of the newest digital technologies which must be taken under consideration in making the governmental policies.

3.1. Among the main benefits of applying blockchain technology in governance

- Low economic costs, time and complexity in the exchange of information between governments and between the public and private sectors that improve the governments' administrative functions.
- Increasing transparency, automation, accountability and auditability for information in government records for benefits of the citizens.
- Reducing bureaucracy, discretion and corruption resulting from utilizing contracts.
- Increased confidence of the citizens and businesses in the governmental processes and record keeping, which are driven by using algorithms which aren't regulated by governments anymore.
- Blockchains have a potential for the facilitation of the direct interactions between the citizens and the public institutions.
- mproving public services in recording transactions and exchanging operations.

Blockchain is a combination of many existing technologies, but it constitutes an efficient, decentralized and informational infrastructure that is reshaping the way in which governments and citizens interact with each other. Blockchains have the ability of reducing the operational risks and transaction cost, increasing the compliance and trust in the governmental institutions. On the other hand, the lack of stable and mature trading platforms and the presence of some gaps in basic functions indicate the lack of actual applications within the government. Decentralization comes in the form of blockchain, but the key disadvantage of block chains is their lack of scalability. Blockchain relies on intensive consensus mechanisms, which leads to more processing costs and increased energy consumption [22-24].

4. A comparison between the structure of e-governance before the emergence of the blockchain and after- emergence of the blockchain (proposed system)

4.1. E-governance before the emergence of the blockchain

Old government systems rely on traditional databases with a structure (client - server). The client represents the citizen or the beneficiary, and the data is stored on a server. The database is controlled with a certain authority that validates customer data before providing access to the database. The central authority is responsible for managing the database represented by adding, deleting, modifying and updating.

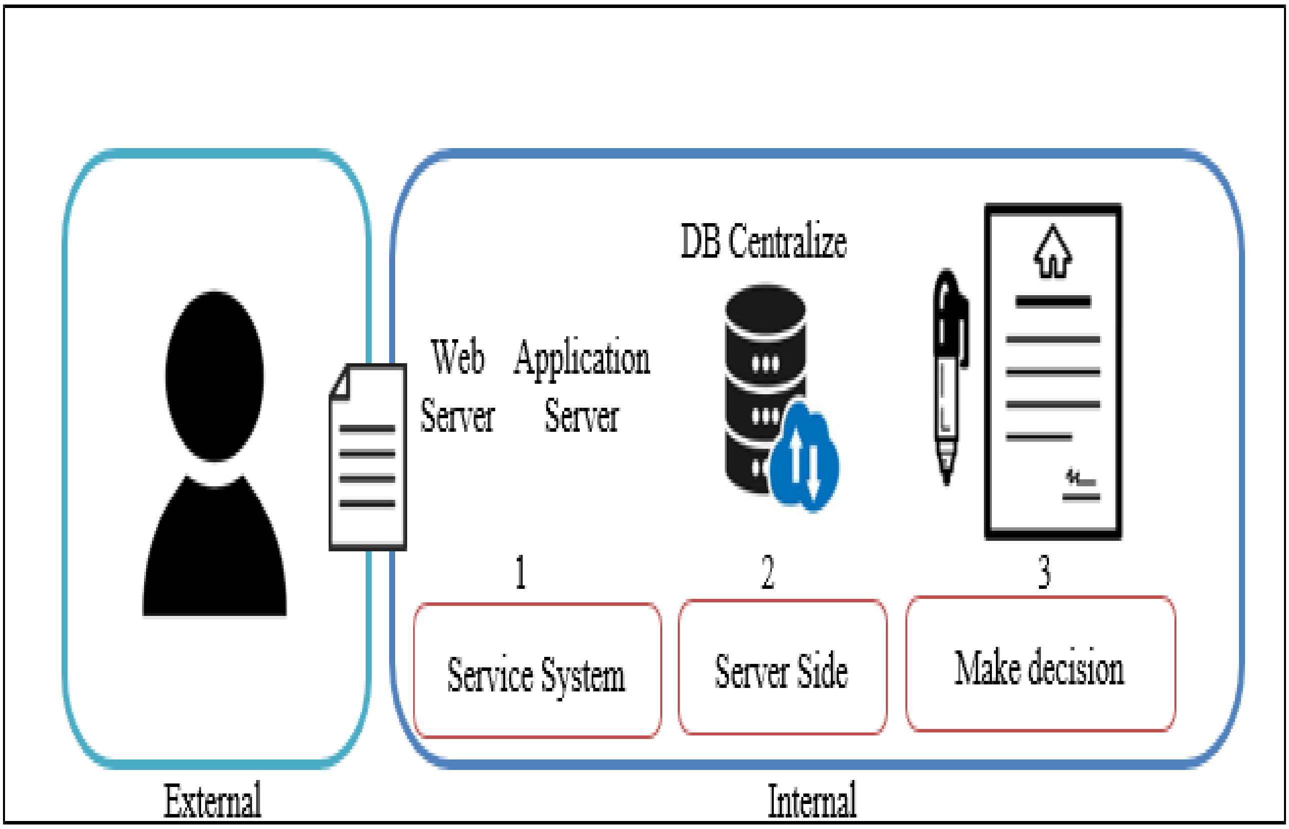


Figure 4. Implementing e-governance without blockchain technology

Figure 4 shows us the application of e-governance without blockchain technology, the work is summarized in several operations:

Service System: It is a set of operations, including (requests submitted by the citizen or the beneficiary party) It must be submitted in person by the citizen or via the Internet. The request is passed through a series of procedures, including archiving, inbox, and administration and then pass the request to the system.

Service Side: It is the examination of the request submitted through the central database (that any decision-making will be in the hands of one authority and in the hands of one citizen).

Make decision: Represents the output and print the contract after making the decision.

4.2. B-E-governance after the emergence of the blockchain (proposed system)

E-government services have evolved significantly over the past decade from traditional paper-based procedures to digital services. Where transactions are processed electronically while providing integrity, confidentiality, transparency and providing response times. Blockchain has all these characteristics to provide stability and transparency of transactions and help in providing trust between nodes.

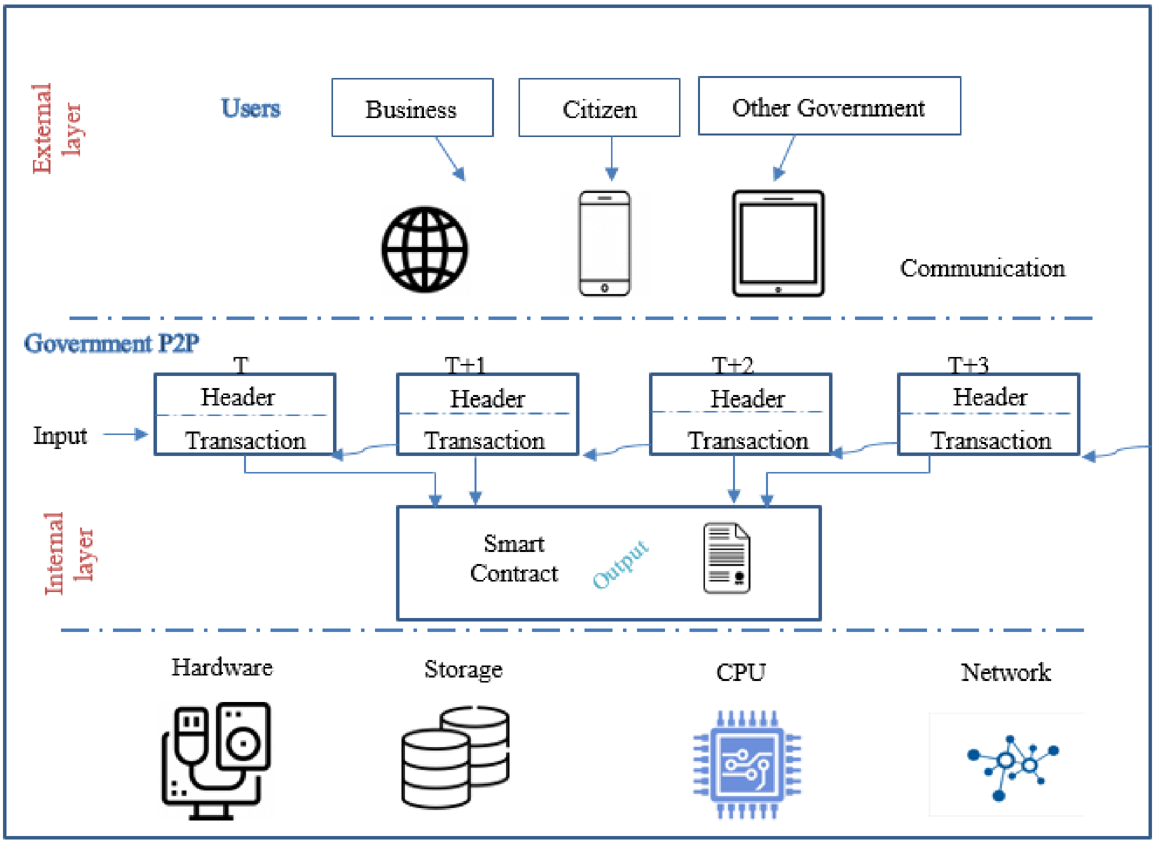


Figure 5. Implementing e-governance with blockchain technology tion, decentralization and distribution

Figure 5 shows us a proposed system for building electronic governance based on blockchain technology.
The system is summarized in two parts, internal and external.
External layer: - It consists of the information of the user of governance, and the second layer of the Internet is accessed through electronic devices or smart phones, through which the internal layer is dealt with.
Internal layer: - It is represented by the blockchain layer and refers to a group of auditors who are responsible for verifying and authenticating transactions before adding any transaction to the block. Investigators are obligated to collectively sign transactions, either granted by contract or rejected. As for the last layer, it is represented by a set of technologies represented by the network, storage of physical materials, etc. The network is to provide communication between users of the e-government and the blockchain layer, such as Wi-Fi, Ethernet or the cellular network. The Storage represents the storage and replication of data such as images and PDF files. It cannot be stored in the block-chain, and it cannot be deleted or changed. Rather, it is an appending rule that cannot be deleted or changed, and this is considered the most important layer. The system was applied to one of the affiliated government departments for the directorates of Baghdad municipalities. The system is distributed and used between more than one nodes. Each node has access to this system. The work of the directorate is to give contracts to citizens proving their ownership of the state, whether they are beneficiaries of the state a plot of land or not. The database has been stored with the names of citizens Beneficiaries of the state by SQL server, MongoDB and stored in the cloud. Previously, the process was traditional, which is the withdrawal by mail of requests, then they are transferred to one node to make a decision about them, with that decision in the hands of one node, and there may be corruption or manipulation of the results for the benefit of the node or for the benefit of the citizen. As for the proposed new system, the database upload it to the cloud,

and a decision will be taken by all the participating nodes registered in the system. The system is scalable and more flexible as it is possible to add new nodes or delete node and assign it tasks without affecting the work environment.

5. The scenario used for deciding on a transaction proposal

The first stage: a request is submitted by the citizen. The request is (the extent to which the citizen has benefited from the state), i.e. proof of the citizen's ownership of the state. The request is a letter supplied by another Directorate or submitted by another department, or the request may be personal by the citizen himself.
The second stage: The submitted application will be passed in several stages and several node.

- First Node: - the transaction will be examined if the transaction has been submitted previously or not. If it was submitted previously, the answer will be given immediately. If it was not submitted previously, a new transaction will be opened in the name of the citizen. The transaction includes recording all the citizen's information and submitting the application as a pdf and pass the transaction to the second node.
- Second Node: - add information about the proposed transaction and pass it to the third node.
- Third Node: - The third node adds some details and information about the citizen. The transaction is passed from the third node to the first node for archiving.

Withdrawal of the benefit, and we mean by it if the person whose name is among the beneficiaries or not, it will be automatically from the data base and the contract does not interfere with that
The third stage: A contract is opened for a citizen. The contract is in two forms, either beneficial or non-beneficial ,if he is a beneficiary, his benefit from the state is proven by the part number and county with the installation of a digital signature for the nodes participating in the previously used mechanism, which proved that the citizen benefited from the state. Figure No 6, shows us that the request submitted by the citizen has been submitted previously, so the first node provides the citizen with the contract. As for the figure No 7, it shows that the citizen submitted a new request, which was submitted for the first time. In the event that the request is suspicious of the form that has been transferred to it, can refuse the submitted request, and no movements will be recorded in the blockchain.

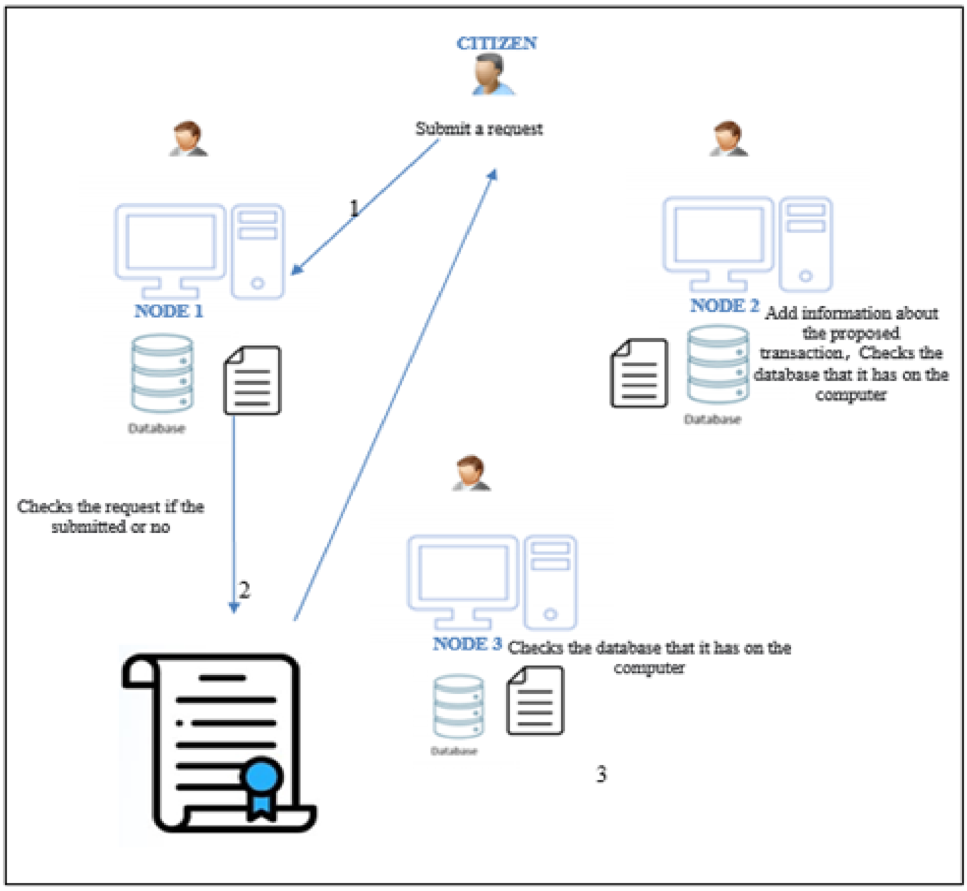

CITIZEN
Submit a request
1
NODE 1
Database
Checks the request if the submitted or no
2
NODE 2
Add information about the proposed transaction, Checks the database that it has on the computer
Database
NODE 3
Checks the database that it has on the computer
Database
3

Figure 6. Submit a transaction and prove that it was submitted previously

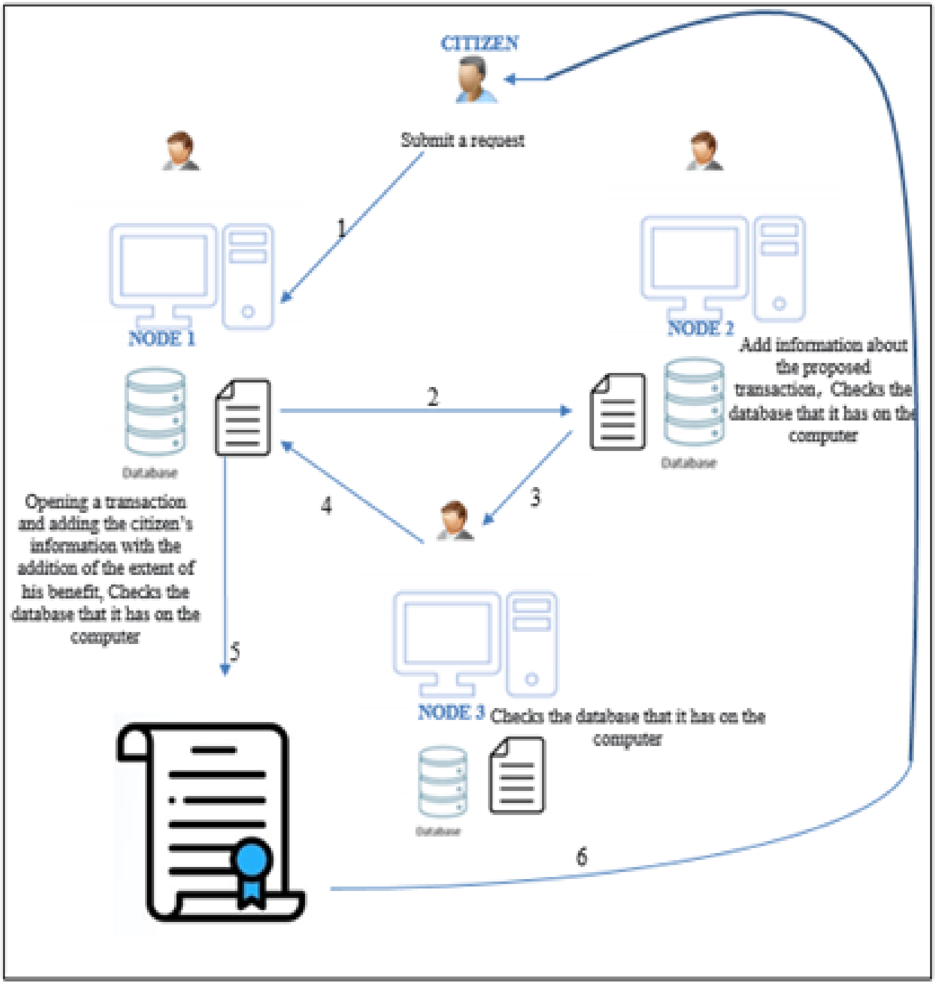

CITIZEN
Submit a request
1
NODE 1
NODE 2
Add information about the proposed transaction, Checks the database that it has on the computer
2
Database
Database
Opening a transaction and adding the citizen's information with the addition of the extent of his benefit, Checks the database that it has on the computer
4
3
5
NODE 3 Checks the database that it has on the computer
Database
6

Figure 7. Submit a new transaction that was not previously submitted

Any transaction passing from one node to another will be stored in the blockchain. It is not allowed to pass any transaction except after verifying that the node is registered in the system by generating a hash for the transaction. So, each transaction will have a series of moves, with all the hash resulting from these moves being recorded. After the citizen's information is obtained from the data base and his transaction is filled out by the node participating in the system. A private smart contract is opened for the citizen. It turns out that the smart contract will contain a QR CODE for each transaction. The QR CODE is the result of the signatures of all node. The signatures here are generating a hash for each node (each node filling in its own fields is converted to a hash) and finally, the generated hashes are collected and converted into a QR code. The last stage, when withdraws the validity of the issuance of transaction citizen, a recovery of the QR-CODE is done, and thus the node will extract all the details of the transaction with all its movements and smart contract.

6. The system analysis

Proposed system was analyzed in terms of strengths, which are represented by several steps that included:-

6.1. The time of raising the transaction request

The time taken to open a transaction by the node is in real time.

Table 1. The time taken to open a transaction

Node	Time Execution
Node1	0.00

6.2. The ease or complexity of the system

The suggested system is a system that enjoys ease of use and flexibility.
The most useful feature is that the system has the ability to add and delete nodes and open interfaces, as a work has been done for the system so that we do not need to reprogram the system again.
But as the internal programming of the system, it is very complex to prevent any attack that may affect it.

6.3. Dependence of performance on the number of transactions per second

The performance of a blockchain network is dependent upon the number of transactions processed each second. User transactions are verified in one second or less, and the increase in the number of validators in a network will reduce the speed. Therefore, the presence of a sufficient number of validators provides better verification of transactions.

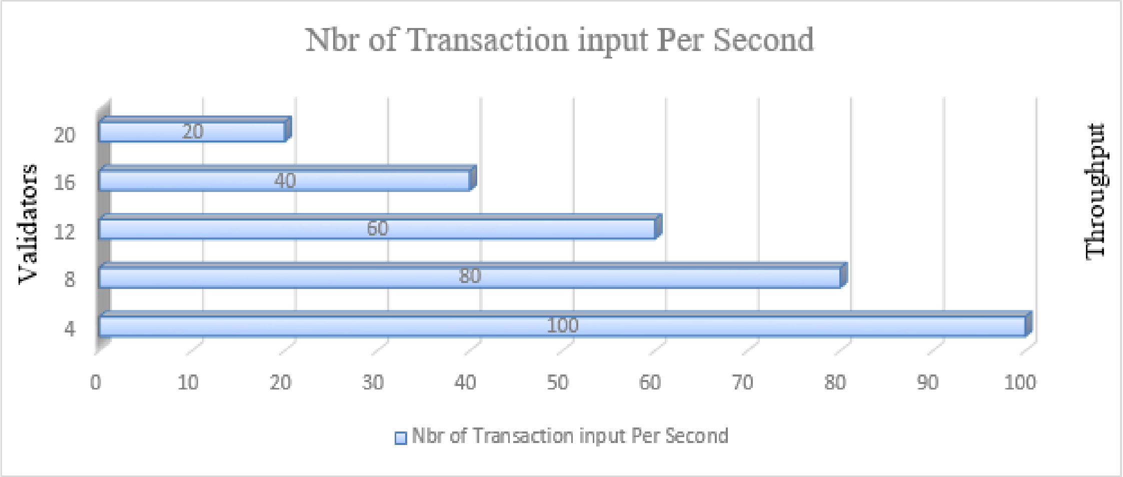


Figure 8. The number of transactions per second against validators. Decentralization and Distribution

A network of 1, 2, 3, 4 and 5 validators can validate a large number of transactions in less than a second. Whereas, if the number of auditors increases, the time required to audit transactions may increase from the ideal limit.

6.4. The capacity, which is represented by the size of the network bandwidth

Maximum data transfer rate over a given path
Bandwidth = number of transactions per second=TPS
TPS equation has two constraint / variables:-
Block size =A
Block time =B
TPS= (block size)*(block time)
= (transaction / block)*(block/ second)
Block size= 2500 transaction/1 block
Block time =1 block /3000 min = 1 block/ 180000 sec
TPS= (2500/1)*(1/180000) =2500/0.00000555=450.004
Blockchain=E-government
Blocksize: 2500transaction
Block time (speed) =1/180000 sec
Capacity = 450.004 TPS

6.4. Transaction throughput

The read transfer rate measures the number of read processes that are completed in a specified period of time. It is represented in readings per second as follows:

Throughput= total read operations/ total time in sec.

The transaction transfer rate represents rate at which valid transactions are executed by a block-chain in a specific period of time, and it does not represent the transfer of the transactions in one node, but in all nodes.
Transaction throughput = total committed transaction/ total time in second

Table 2. The time it required to implement a number of transactions

Number of transactions	**Time execution**
100	2 hour – 120 min -7.200sec
500	10 hour – 600 min -36.000 sec
1500	20 hour – 1.200 min -72.000 sec
2500	50-hour-3.000min-180.000sec

6.5. Transaction latency

The transaction response time is a network-wide display of amount of the time that it takes for the effect of the transaction to become usable over a network. The measure comprises the time that it takes from the point at which it’s presented to the point at which result is commonly available in a network. And that includes the time of the propagation and any settlement time as a result of consensus mechanism in place with it.
Transaction response time = confirmation time - submit or dispatch time

6.6. Security and privacy assessment

A qualitative assessment of how the proposed system prevents external threats from attacking DDOS that occur when attackers attempt massive Internet traffic with bogus requests to render the service unavailable. Thus, it will consume a large amount of bandwidth and resources, which will lead to disruption of the service. The solution is not to use a central server, but the load must be distributed on the network.

6.7. Authentication attacks

When users try to control the network so that they can delegate themselves or provide a contract to delegate users while they are in control. This is considered impossible in the system because all the nodes have been selected in advance with the possibility of specifying the tasks they perform. In the proposed system, any adversary trying to contact the system will be detected, and users who are trying to access information will be verified. Some of the advantages of the proposed blockchain are summarized.

- Transaction speed: Only a group of participants processes transactions.
- Scalability: New participants can be added to the system.
- Low transaction costs: - Verify transactions without fees to the citizen.
- Low energy consumption: A simple verification mechanism has been used with low energy consumption.
- Attack 51%:- Low risk of 51% Random participants are not allowed to join the network and nodes are specified in it before and it is not allowed to give tasks to a node more than a second All nodes are equal.
- High transparency: Participants in the network know their peers. There is a high level of cooperation so that departments can share information upon request.

7. Conclusion

In this research, an e-government structure was proposed based on the blockchain technology, through which the transaction is evaluated based on the number of transactions per second. It is possible to keep fewer validators for higher throughput of transactions. Through the system, we demonstrate the architecture to provide security, privacy, transparency, and less risk from external attacks.

References

[1] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper,* vol. 3, no. 37, 2014.

[2] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *arXiv preprint arXiv:.00858,* 2020.

[3] T. Tian, "Social Big Data: Techniques and Recent Applications," *International Journal of Computer Science Security,* vol. 14, no. 5, pp. 224-235, 2020.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review,* p. 21260, 2008.

[5] N. Aburumman, J. Fraij, and R. Szilágyi, "Digitalization: The Use Of Blockchain In Public Sector," *Oradea Journal of Business Economics,* vol. 5, no. 2, pp. 72-82, 2020.

[6] H. Salim, and N. Alseelawi, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International journal of online and biomedical engineering,* vol. 18, no. 3, 2022.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress),* 2017, pp. 557-564: IEEE.

[8] H. Alrikabi, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021.

[9] R. BACCOUR, "Analysis of financial transactions in Bitcoin," *République Tunisienne,* 2016 - 2017.

[10] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.,* vol. 19, no. 5, pp. 653-659, 2017.

[11] J. Kietzmann and C. Archer-Brown, "From hype to reality: Blockchain grows up," *Business Horizons,* vol. 62, no. 3, pp. 269-271, 2019.

[12] W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.

[13] R. A. Azeez, M. K. Abdul-Hussein, M. S. Mahdi, and H. T. S. ALRikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2021.

[14] S. Davidson, P. De Filippi, and J. Potts, "Disrupting governance: The new institutional economics of distributed ledger technology," *Available at SSRN 2811995,* 2016.

[15] T. F. Bresnahan and M. Trajtenberg, "General purpose technologies 'Engines of growth'?," *Journal of econometrics,* vol. 65, no. 1, pp. 83-108, 1995.

[16] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," *Communications of the ACM,* vol. 63, no. 7, pp. 80-90, 2020.

[17] P. Baran, "On distributed communications networks," *IEEE transactions on Communications Systems,* vol. 12, no. 1, pp. 1-9, 1964.

[18] R. Beck and C. Müller-Bloch, "Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization," 2017.

[19] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access,* vol. 7, pp. 36500-36515, 2019.

[20] H. Workie and K. Jain, "Distributed ledger technology: Implications of blockchain for the securities industry," *Journal of Securities Operations Custody,* vol. 9, no. 4, pp. 347-355, 2017.

[21] S. Kumagai, S. Bandyopadhyay, and H. Grandvoinnet, "Mainstreaming Citizen Engagement in Public Financial Management for Better Results," 2019.

[22] D. Allessie, M. Sobolewski, L. Vaccari, and F. Pignatelli, "Blockchain for digital government," *Luxembourg: Publications Office of the European Union,* 2019.

[23] S. AS, M. AM, A. Adegboyega, and O. Odeniyi, "A Framework for Participatory E-Governance System."

[24] A. Razzaq, M. Khan, R. Talib, A. Butt, N. Hanif, S. Afzal, and M. Raouf, "Use of Blockchain in governance: A systematic literature review," *International Journal of Advanced Computer Science Applications*, vol. 10, no. 5, pp. 685-691, 2019.