

Data retrieval based on the smart contract within the blockchain

Zainab Ali Kamal ¹ and Rana F. Ghani ²

^{1,2}Computer Sciences Department, University of Technology-Iraq, Baghdad, Iraq

ABSTRACT

Blockchain technology appears to be the ideal solution for storing data in a transparent and decentralized manner. It also allows open access to data and enhances its immutable nature. This technology has helped prove its usefulness in several industries so far, however, distributed ledger technology does not work as a pure database. Therefore, some problems occur in accessing data. Querying data in the blockchain leads to performance and bandwidth problems. This primarily occurs because the blockchain does not have a primary query language, unlike regular databases. The distributed nature of the blockchain is in this case an obstacle. In this paper, a safe and fast method will be proposed to retrieve consistent data from the blockchain-based on the smart contract that will be opened after completing the transaction procedures. All nodes will sign the proposed transaction (by adding a special hash to each node resulting from the transaction information and node data). Upon completion of Transaction procedures, A smart contract will be opened (in which a QR is placed) resulting from converting the signatures in the transaction to QR When the smart contract data is retrieved, the QR for each transaction will be used All node signatures and transaction data will be extracted . The data will be retrieved by the QR generated for each transaction after it is stored in all nodes servers participating in the system. A new method was proposed to generate a hash for each node present in the system. The proposed method was tested in terms of time and complexity, and the algorithm was statistically analyzed, and all the results proved successful.

Keywords: Blockchain, Smart Contract, Big Data, and Store Data

Corresponding Author:

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

1. Introduction

Transactions are made between the parties in centralized systems that require a trusted third party but lead to a single point of failure and high transaction fees and Data is constantly growing in the era of big data, although there are many benefits related to the use of big data as a major resource for the economy, at the same time, there is a growing concern about user privacy and misuse of user information. In this context, blockchain technology has emerged as a promising technology to enable appropriate data management using the concept of an independent updated general ledger by each participating party in the network. This technology was used to address these issues by allowing untrusted entities to interact with each other in a distributed manner without the involvement of a trusted third party [1, 2]. The architecture of the blockchain makes it immutable and transactions cannot be tampered with. Once they occur, they are formally validated and recorded in a chain of blocks. Based on blockchain encryption, eliminates the need for a trusted third party, allowing the implementation of reliable and powerful applications. Blockchain has been used for cryptocurrency in addition to its use in a wide range of fields [3]. One of the advantages that this technology provides is consensus to ensure that transactions are not changed, reversed, or canceled, despite all these features discussed, there are new challenges in data management and retrieval. Data is stored in permanent and transparent blockchains for the entire network. This leads to governance issues to ensure data

© The Author 2021. This work is licensed under a [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/) (https://creativecommons.org/licenses/by/4.0/) that allows others to share and adapt the material for any purpose (even commercially), in any medium with an acknowledgement of the work's authorship and initial publication in this journal.



quality [4]. Data needs consistency to define data recovery goals. A consistent database contains successful results, and in this case, it is called a consistent attribute or a logical constant. Transactions need consistency so a consistent update of the database file will be created. We conclude that retrieving data from consistent transactions will be easier and faster if the transactions are inconsistent [5]. Through this research, we will deal with the privacy concerns that users face when retrieving data. We will focus on Windows applications for government agencies. These apps collect high-resolution personal data. These services are honest but intriguing. This system may be used for other data privacy concerns. The system needs to be protected from several problems, the most important of which are: Corruption. If the application is under the command of one employee, the employee can decide the citizen, which is a wrong decision in favor of the citizen (as a result of bribery). We need smart contracts in which all employees participate to make the final decision. When retrieving citizen data from the blockchain, it will be based on the smart contract shared in its decision, a group of employees with the citizen himself, safely and easily. This research is divided into the following sections:-

(II) Introduction to blockchain technology.

(III) Smart contract in the blockchain. (V) Big data and retrieve data. (IV) The last section describes how to retrieve data from the blockchain in a fast and secure manner.

2. Blockchain technology

Blockchain technology is not just one technology, but rather a combination of technologies such as encryption, mathematics, and algorithms such as consensus and distribution algorithms [6]. Blockchain is the basis for proposed applications in almost every sector. These applications are designed to remove rent-seeking companies from digital operations while giving users more control over their data. Blockchain offers a new type of shared database. The blockchain-based database is replicated on multiple computers. Bitcoin's success has proven that blockchain technology is useful for projects that require real-time collaboration between questionable contributors [7]. The basic premise of the blockchain is to build trust in a peer-to-peer network without the need for an external third party, such as Bitcoin. When transferring a monetary value, it does not need a bank or other financial institution to carry out the transfer. Transactions are stored in chain series of a data structure called blocks and each peer in the blockchain network is called a distributed ledger and is updated at the same time [8, 9]. So, blockchain systems consist of two main types:

-A peer-to-peer network is the mechanism operated by many computers.

- The database stores the complete file of the transaction history and the order in which the transaction occurs. The blockchain is the same as the database. The database is created by transaction history. In the beginning, the first block is called genesis Block, and everyone agrees on it. Then people start submitting their transactions and broadcasting them through the peer-to-peer network. New blocks will be added to the network that brings transactions together. By doing this, it will establish a consensus on the order in which the transaction was made, and an encryption process will be carried out, a signature will be added to the end of the block, and a link will be created to the previous block [10, 11]. Blockchain technology can be considered a complex process. The reasons may be the complex interaction of the elements of the blockchain and as a result of the characteristics that are difficult to understand in detail and the lack of strong common knowledge to the basic building blocks of the blockchain:

Cryptography: This technology depends mainly on encryption and electronic signature of operations through which the identity of the user is determined and permission for persons who have the right to access information and this technology contains three main elements (The hash is a unique code - a public key cipher - a digital signature). **Consensus mechanism:** It depends on what is known as the synchronization of records to ensure that a new process is added to the correct chain and does not contain contradictory information. This process is called mining. **Datastore:** It is an electronic ledger in which all operations of the blocks are combined using consensus algorithms, and each block is linked to the previous one.

Peer-to-peer network: is the network through which information is transferred and exchanged without the need for a third party. **Nodes:** The user or computer involved in the blockchain [12, 13]. Simple processing is done to create a hash for the transactions that take place. It is impossible to perform a reverse operation to retrieve the actual data once the hash data is known [14, 15]. Once a new block is created, functions are used to confirm the block. Each block is connected to the previous block with a hash value. If someone wants to change the value of the data, the hash value will change. It is possible to detect the hiccups when an intruder

occurs and changes blocks in the blockchain [16]. Current SHA algorithms consist of SHA1, SHA2, and SHA3. SHA differ from each other in the number of bits, for example, SHA224, SHA256, SHA384, and SHA512 [17-19].

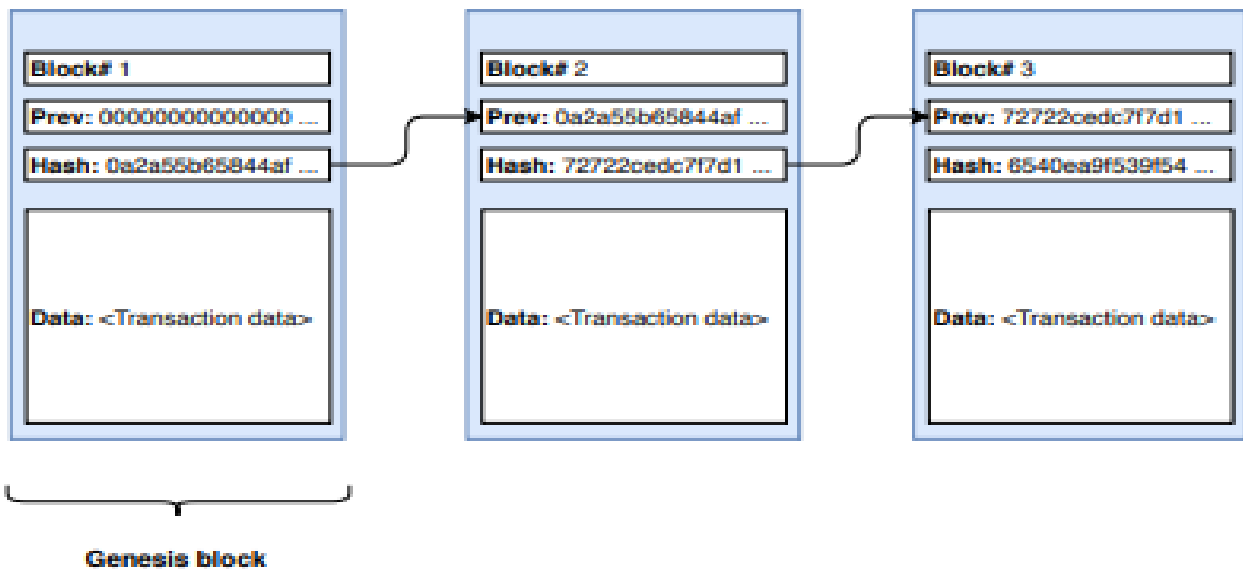


Figure 1. Hashing chains the blocks together and renders them immutable [20]

3. Smart contract

They are programs stored on the blockchain that is run when pre-set conditions are met. They are usually used to automate the implementation of the agreement so that all participants can immediately be sure of the result without the intervention of any intermediary or loss of time. They can also automate the workflow, causing the next action to run when conditions are met. Smart contracts work by following phrases IF/When. Then that is written in the blockchain. A network of computers performs actions when predefined conditions are met and verified. These actions can include disbursing money for taxes, registering cars, sending notices, or issuing a ticket. The blockchain is updated when the transaction is completed. This means that the transaction cannot be changed and only the parties that have granted permission can see the results.

Within the smart contract, there can be as many conditions as needed to satisfy the participants that the task will be satisfactorily completed to create the conditions. Participants must determine how transactions and their data are represented on the blockchain and agree on rules IF/When Then that governs those transactions, explores all possible exceptions, and defines a framework for resolving disputes. The purpose of smart contracts is to facilitate transactions between actors who do not know each other and to ensure that each contracting party fulfills its obligations and avoids any fraud. This reduces payment delays and the risk of error, but it also avoids potential friction over contract terms and mutual obligations. But the safe and intelligent nature of these protocols does not leave room for hesitation or interpretation, as contracts must be implemented on specific and acceptable terms without the possibility of bypassing the system [21, 22].

3.1. Advantages of smart contract

- Speed, efficiency, and accuracy: - Once the conditions are met, the contract is executed immediately, since smart contracts are digital and automated, there is no paperwork to be processed, and no time is spent resolving errors that often result from manually making documents.
- Trust and Transparency:-Since there is no meaning of a third party and because records are encrypted for transactions that are shared through participants, there is no need to ask about whether the information has been changed for personal benefit.
- Security:- Transactions are encrypted, making them difficult to hack. Since each record is connected to the previous and subsequent records in a distributed ledger, it is difficult for hackers to alter the entire chain to change a single record.

- Conservation:- Smart contracts eliminate the need for intermediaries to handle transactions, so time delays and fees associated with transactions do not exist [23, 24].

3.2. Big data and storing data

Big data has several advantages of volume, velocity, and variety, and veracity, here are the features of Big Data:

- Volume: Big data processing usually faces challenges that include stereotyped curses (storage, data loading, and different data distribution). The curse of dimensions (which contains many features and attributes)
- Variety: Diversity represents different types of data such as video, text, and audio that generally consist of structured data, semi-structured data, and unstructured data. The complete data cannot be stored in the data center, but it is usually distributed over a large number of sites. The heterogeneity of data is distributed from different sources.
- Velocity: The Velocity of data generation (that is, how quickly the data is generated).
- Veracity: Veracity refers to the quality aspect. Data can be collected from multiple sources, including low-quality and noisy samples. Data can be generated by broken or unreliable Internet of Things devices. To improve the quality and analytical accuracy of big data, it is a challenge related to big data analytics, which is to extract useful information and patterns from a data set that is used for different files.

Governments and private organizations are investing in big data and blockchain technologies due to their great ability to solve many real-world problems.

Customers are more inclined to transact online and an increasing amount of data is generated every day.

This exponential rise in digital data generated creates new opportunities for industries to understand customer needs and customer trends. Big data set analysis plays a major role in gaining insight into customer patterns. These challenges can be addressed through the unique properties of the blockchain such as decentralized storage, transparency, and compliance mechanisms. The information is stored in the blockchain in any way requested by the application. Usually, a single blockchain storage model is not implemented. Concerning the actual data of the blockchain, there are common options represented by:-

- Plain: The data can be read by anyone with access to the blockchain and uses a simple approach to facilitate data validation and provide data transparency.
- Encrypted: It can be read by people who have access to the key required to decrypt. If encrypted with a private key, decryption with a public key can act as a form of signature to ensure that data is added by a particular party.
- Hash: Information is stored only in the blockchain, and the original data is stored elsewhere. The data can only be accessed by the important participants. In this case, the blockchain acts as a tool to ensure that the data is not modified by keeping the hash extension as an immutable source.
- Pointers: Instead of storing data, a pointer is stored for it, which can be an address URL or a file. And a query SQL is made to be executed in a pre-defined database or anything else that the system developers can access [25]. So, the blockchain is not a place to store all kinds of different data. It is a file or record in which transaction records are kept. A transaction can be a record of any transaction and may contain any type of data. The transaction can be linked to cloud storage and data can be stored in different formats [26]. Data storage solutions have been developed to solve scalability. Databases have become more complex with the ever-increasing use of various types of data, big data, and cloud infrastructure. The data needs data management models such as relational and non-relational. Non-relational is common for the increased storage of unstructured data and the increased use of machine learning. The blockchain architecture is a non-relational database. The blockchain system called Post chain appears to be the first system to use the relational model that gives general characteristics to decentralized solutions with relational databases. Consistency is difficult and expensive to achieve in relational databases when there is more than one party. All nodes in a blockchain must have complete copies of the dataset, and security services such as availability, integrity, and fault tolerance are greatly supported by blockchain systems. Users trust databases, but no one can be sure of that because administrators have complete control over the systems. Even competing companies need to share data, and they do not need to build trust among themselves, but they must trust the shared data. Blockchain

systems guarantee trust without the use of intermediaries, and trust is created using an independent code and two consensus protocols. Thus, decentralized solutions are more suitable for big data operations. Relational databases generally handle small data better, while decentralized solutions handle big data better [27].

4. The proposed system

Many government departments and organizations require their citizens to issue their certificates and credentials. The citizen is obliged to refer to the department from which he issued a card or a document that was a certificate, document, or identity, and ask the concerned authority to validate the issuance.

At the same time, the employee should review the citizen's archive to give him the validity of the issuance of the document. The proposed system is a system shared and distributed among more than one employee, which will pass through several stages represented by:-

- The stage of opening transaction a form for the citizen.
- The stage of deciding on the transaction and give a contract to the citizen.
- Data Retrieve stage.

4.1. The stage of opening transaction a form for the citizen

The form goes through more than one employee to fill in the citizen's information

For example, the first employee fills in the citizen's information in addition to filling in information about the employee himself. The second employee, when the form is passed to him, gives the form an incoming number and fills in the employee's information. The third employee searches for the citizen's information if it is within the database or not to transfer the form to the second stage. But before the transaction is sent to the second stage to open a contract for the citizen. Each time the employee fills out the information on the form with his information, a hash is generated for each employee. The hash obtained from each employee and the citizen's form information is collected and transferred to the QR.

4.2. Generating Hash function steps

1- Convert the employee data to be filled into bits, the message is broken into chunks of 1,024-bit blocks.

If the data is less than 1024 bits, it is expanded by using chaos theory 1D, Only 4 numbers are taken after the (.) .the numbers mod 256 are placed in a buffer and then convert to Binary

$$r_n = t(1 - r_{n-1})r_{n-1}$$

where $t \in [0,4]$, $r_n \in (0,1)$, and $n \in N[22]$

2- Compress data from 1024 bits to 512 bits based on primitive polynomial (compression 32 words (consist 32 bit each word) to (32 words (consist 16 bit to each word)

3- 512 bits are divided into two parts (right and left),

Each part contains 256 bits. Each of the right and left parts will contain 8 words, each word consists of 32 bits, word= a,b,.....h.

4- At the same time that the citizen's data is withdrawn, the data recorded in the citizen's form is withdrawn and transferred to Binary

If the data is less than 1024 bits, it needs to be expanded base on chaos theory 1D and divided into.K0 to K32, each K contain 32 bits.

5- SHA 2/256 bit. Logic is used/ repeat 32 round

$$T1 = \Sigma(e) + ch(e, f, g) + h + k0$$

$$T2 = \Sigma o(a) + maj(a, b, c)$$

$$Ch(e, f, g) = (e \wedge f) \text{ xor } (\neg e \wedge g)$$

$$\Sigma(e) = e \ggg ROT6 \text{ XOR } e \ggg ROT11 \text{ XOR } e \ggg ROT25$$

$$\text{MAJ}=(a \wedge b) \text{ XOR } (a \wedge c) \text{ XOR } (b \wedge c)$$

$$\sum o(a) = a \ggg 2 \text{ XOR } a \ggg 13 \text{ XOR } a \ggg 22)$$

6- Update buffer into left and right

The logic operations are repeated 32 times to get 2 hashes,

$a = T1+T2, b=a, c=b, d=c, e=d+t1, f=e, g=f, h=g$

7- XOR between (left and right) given 1024 bit convert and to QR

Algorithm: generate hash-QR

Input: Employee and citizen information

Output: QR

Begin

Step 1: The message is broken into a chunk of 1024 bite blocks.

If blocks less than 1024 bit

Made Expansion message, x [1024] bite by Chaos 1D generated random number.

Step 2: Compress data from x[1024] bits to x[512] bits

Step 3: divided 512 bits into two parts (right and left),

Each part contains 256 bits.

Each of the right and left parts will contain 8 words, each word consists of 32 bits, word= a,b,.....h.

Step 4: Citizen data transfer on the transaction to bits, if Citizen data less than 1024 bit made expanded, x [1024] bite by Chaos 1D generated random number.

Step 5: SHA 2/256 bit. Logic is used to left and right part/ repeat 32 round

$$T1=\sum(e) + ch(e, f, g) + h + k0$$

$$T2\sum o(a) + maj(a, b, c)$$

$$Ch(e, f, g) = (e \wedge f) \text{ xor } (e \wedge g)$$

$$\sum(e) = e \ggg ROT6 \text{ XOR } e \ggg ROT11 \text{ XOR } e \ggg ROT25$$

$$\text{MAJ}=(a \wedge b) \text{ XOR } (a \wedge c) \text{ XOR } (b \wedge c)$$

$$\sum o(a) = a \ggg 2 \text{ XOR } a \ggg 13 \text{ XOR } a \ggg 22)$$

step 6 : Update buffer into left and right

$a = T1+T2, b=a, c=b, d=c, e=d+t1, f=e, g=f, h=g$

commutative the result

step 7: XOR between (left and right) given 1024 bit and convert to QR

End

4.3.The stage of deciding on the transaction and give a contract to the citizen

The second stage: A smart contract is opened to the citizen after the final decision is made by the employees by searching for his information in the databases of the system. The contract is given as a QR resulting from the hash generated from the citizen's form information and employee's information.

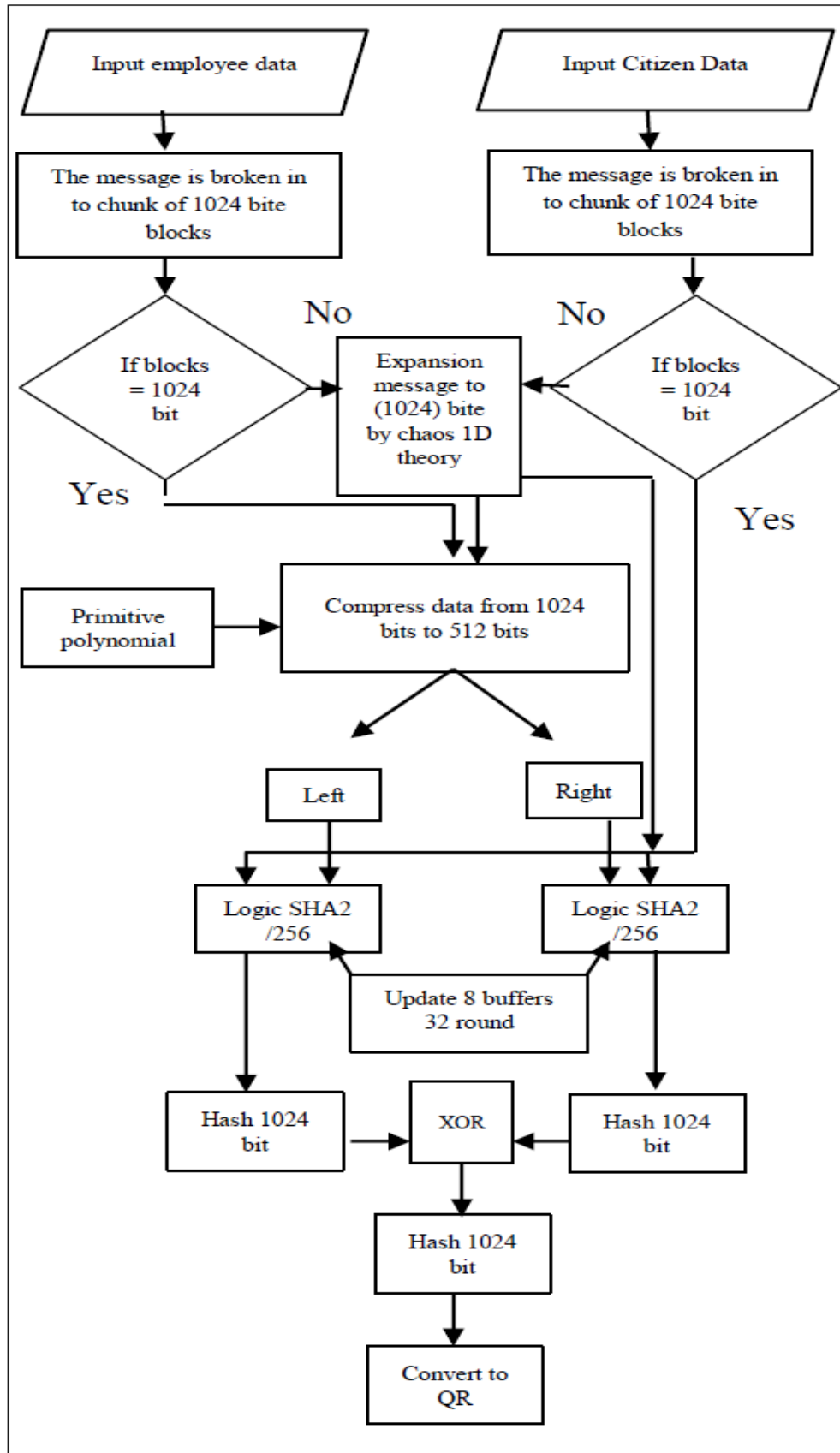


Figure 2. Block Diagram for Propose Chaos - QR

Example:-

1- expansion Message

Input employee data = zainab convert to binary and lack of characters (expanding the to 128 characters) is compensated by generating random numbers from the chaos equation

Zainab convert to binary → 011110100110000101101001011011100110000101100010

Chaos 1D logistic map (generated 100 random numbers), take only 4 numbers after (,) and convert to binary

	Generate 100 random numbers. Take only 4 number after (,) and made mod 256. And convert to binary	
0.3240000000 0.78848645629 0.6003921494143	→	324 mod 256=68 788 mod 256=20 460 mod 256=204

Combine the input message with the result of the chaos 1D and convert it to binary

Message expansion from 48 bit to 1024 bit

```

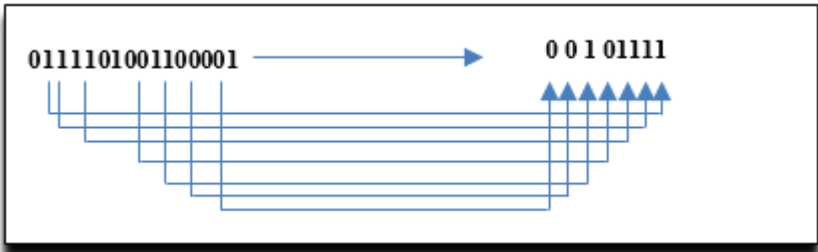
011110100110000101101001011011100110000101100010
0100010000010100110011000010011001111101101001110001001100001
11001110100101001010111101000101001010011101010110000110010010110100010010011100101000011000101101010101010000
11100001010111001110011101000011101100100100010111101110000101101100110000100101010011110001000011111
1101100001101000001110111101100100010000111000101111001011101000101010100010011100001111111000000001010
011000001110011001101100000011100001001110101000101011101010011110100111101101000100110001000010100101111
010110111101011010001000011001000100000010001010100111100100011100001111010111000100000001111001011001100000
0010001111111001111010111100101111010100011011110000111001010111010101000011000010111101000110011101111
01111011001000011000000000101100011010111100000000001011000101111011000010011011100111101011110111011
10111001010111000011111101000010000010111001011011000000010001000101100001100100001010010110010111010100
0100011110011010100110100110100111
    
```

Message expansion HEXA (256 char)

```

7A61696E61624414CC267DA713873A52BD14A756192D12794316DB0E15E73A1D9262FB85D984AA7887F60D03BD910717CB
A2A89C1FE00A60E66C0782758AEA7A7B44C414BD6F5A2191022A791C3EB8807966023FE7AF2F51BE1CAF54182F4677DF6
41800B1AF00162F609B9FAFB95C1FD04172D804458320A597511E6A6967
    
```

- 2- Compression 1024 bits to 512 bit base on primitive polynomial equation: $-x^{15} + x^{13} + x^{11} + x^9 + x^5 + x^3 + x^2 + 1$. 16 bits of 1024 bits are taken at a time. Bit (15, 13, 11, 9, 5, 3,2and 1) are drawn based on an primitive polynomial equation



Message compression (512 bit)

```

0010111111101111101001110000011101010111011111001000110001101000011011000010101101001011000011000001111001011101
1000101001101101000010001111100011011011011011011000110001001000111011000000110111011010111010011100100101001011001
11100100011101011111011110000111100000111101101001010111000001011011011110100100011101101011111100001111101110
00011010100110100001101111010011000110010101100001001111101011000000100101011011001111110101001101000110011010
0011000010111001001100111010100000011110100110101111
    
```


Message compression (128 char HEXA)
 2FEFA703ABBF918D0D85696183CBB14DA11F1B6DB1891D81BB5D39296791D7EF0F03ED2B816DE91DAFE1F70D4D0DE9A32B
 09F5812DD9FD4D19A30B933501E9AF

3- Split 128 char HEXA into two-part :-

2FEFA703 ABBF918D 0D856961 83CBB14D A11F1B6D B1891D81 BB5D3929 6791D7EF	0F03ED2B 816DE91D AFE1F70D 4D0DE9A3 2B09F581 2DD9FD4D 19A30B93 3501E9AF
--	--

Each part divided into 8 word:-

W1: a: 2FEFA703 W2: b: ABBF918D W3: c: 0D856961 W4: d: 83CBB14D W5: e: A11F1B6D W6: f: B1891D81 W7: g: BB5D3929 W8: h: 6791D7EF	W1: a: 0F03ED2B W2: b: 816DE91D W3: c: AFE1F70D W4: d: 4D0DE9A3 W5: e: 2B09F581 W6: f: 2DD9FD4D W7: g: 19A30B93 W8: h: 3501E9AF
--	--

4- Input Citizen Data and expansion

Input Citizen Data = ali, convert to binary and lack of characters (expanding the to 128 characters) is compensated by generating random numbers from the chaos equation

ali convert to binary → 01100001 01101100 01101001

Chaos 1D logistic map (generated 100 random number), take only 4 number after (.) and convert to binary

Combine the input message with the result of the chaos 1D

Message expansion from 48 bite to 1024 bite

```
011000010110110001101001010001000010100110011000010011001111101101001110001001110000111001110100101001010111
101000101001010011101010110000110010010110100010010011110010100001100010110110110110000111000010101110011100
11101000011101100100100110001011111011100001011101100110001001010100111100010000111111011000001101000001
1101110110010001000001110001011110010111010001010100010011100000111111100000000101001100000111001100110
110000000111100000100111010110001010111010011110100111101101000100110001000001010010111101011011101010100
0100001100100010000001000101010011110010001110000111101011100010000000111100101100110000000100011111111001
111010111001011110101000110111110000111001010111010101000001100000101111010001100111011111011101100100000
11000000000010110001101011110000000000101100010111101100001001101110011111010111101110111011101100101011100
00011111101000001000001011100101101100000001000100010110000011001000001010010110010111010100010001111001101
0100110100101100111100011001000111010011100
```

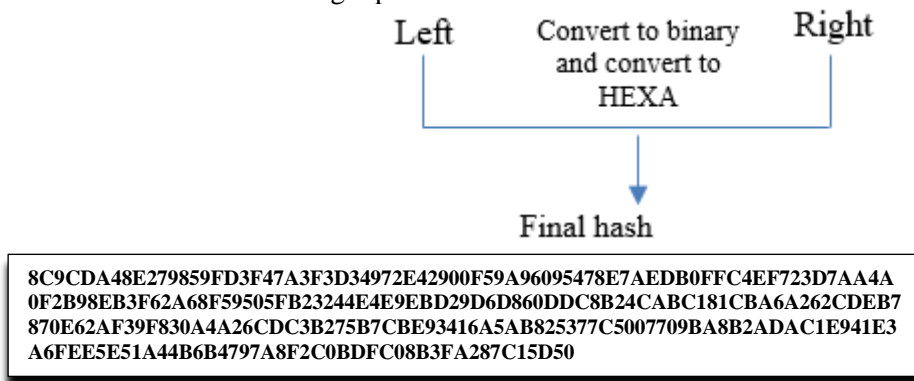
Message expansion HEXA (256 char) 616C6944

```
616C6900A713873A52BD14A756192D12794316DB0E15E73A1D9262FB85D984AA7887F60D03BD910717CBA2A89C1FE00
A60E66C0782758AEA7A7B44C414BD6F5A2191022A791C3EB8807966023FE7AF2F51BE1CAF54182F4677DF641800B1AF
00162F609B9FAFBBB95C1FD04172D804458320A597511E6A69678C8E9C
```

- 5- Logic 256 is used to left and right part with the citizen data/repeat 32 round
- 6- Update buffer

<pre> 19C3735C8A2DD90AC21F3A99B43FC2721D61C201C0E A9CC94049147588E19D5524A74E6E041768B930CBC58A C295ECCBAAF620AB4470BA30593A808F1CF6B6ABF7 FD06222F68173534BF05367C9A54C9F4468231378C5FD3 2631EEEE10629432F59A61417B8461F6B16DB791129A9B 7483EF397F92B42129E63579A97B881F72 </pre>	<pre> 955FA91468545C9511EB40A6890B555C5FF1CD58698A0 98ECE33F9C57725722719DDEACEF6AEE60AC6E1AD7 F579017E88FB86E35F9596CE839E7483D5057772A3C5B A440E2836F45D295F6A9FF901EEF398530448047B6E73 094456C431551328293DBCA515EA01FF08E116FF77F81 30355B40051D982AF626BE460BFC494222 </pre>
--	--

7- XOR between left and right part



8- convert final hash to QR-CODE



NOTE: When passing the transaction to the employees participating in the system, a hash will be generated for each employee shared with the citizen's data, made XOR between hash and last convert to QR-CODE, Hashs are saved in the blockchain with the smart contract that contain the QR.

4.3. Retrieve data stage

The smart is saved with the hash in all servers of the nodes in the network so that it is not adjustable or switchable.

When scanning the QR code, all hashes with the transaction will be retrieved from the node server.

5. Experimental result

The output of the proposed algorithm will be tested according to several metrics, including time, complexity, collision, and statistics tests.

- **Time:** The algorithm (HASH-QR) takes a few milliseconds. The time was calculated using C#'s built-in Timer class.

Table1. The time it takes to generate a hash

Input message	Execution time
Zainab/ali	0.160 millisecond
Mohamed/noor	0.165 millisecond
Waleed/mansour	0.168 millisecond

- The complexity of the proposed algorithm (HASH-QR) will be divided into two stages.
 - The stage of choosing the variables of the logistic equation / in the step 1 and step 4: When changing the values of the logistic equation variables, the entire hash result will change.

Table 2. Complexity in (Hash-Qr) algorithm base on logistic map

message	Initial value (1D)	Output Hash 128 HEXA
Zainab ali	$\mu=3.6$ $x=0.1$	8C9CDA48E279859FD3F47A3F3D34972E42900F59A96095478E7AE DB0FFC4EF723D7AA4A0F2B98EB3F62A68F59505FB23244E4E9E BD29D6D860DDC8B24CABC181CBA6A262CDEB7870E62AF39F83 0A4A26CDC3B275B7CBE93416A5AB825377C5007709BA8B2ADAC 1E941E3A6FEE5E51A44B6B4797A8F2C0BDFC08B3FA287C15D50
Zainab ali	$\mu=2.9$ $x=0.9$	B1B2651D7D062592F05E30E6EB438A8A0A257201E2545193CE79E 91DD8C0D92591EED9FCAECCECF4F779496C023A8B75E2532F 3935D281C89161541330AE7F1FFDFC9E761EBDD1B124EE03A5FE 727237A61FB1A6E825D76F0D8ED304D074EFE320EE9415C267AC BCFB82F12C47269AB04C806FAB3E3F6DD21FD36A7E01279B6
Zainab ali	$\mu=1.6$ $x=0.3$	09DD2B6CD3298E10712E3FE44489716BB29774AC9036A814BEC9 EDA40354D60101E630A33BB0D31805871EA62EBBA1176DD5D5A4 867D53C862B538C841939E267AE6723321551B6829FCC466343A5B C172DC56EB651A5738CC67CDA26452548F9502410826209B4ED9C 00B4C17A0C5D530A7AD24BDE86AA2BD7232C05B070901
Zainab ali	$\mu=2.1$ $x=0.1$	AFCAC4C57590B989D31DA5B5BB376699D717B2AC2AA0A7173 0D0E4E73CCA33F93CA19EC02F970446E7C9F786705618FC1591 F7DE2C9AA9B228C5148F681E2D388DE42A0B738CDFD8939298 D77AE324BEB3C53148B2FDA0E109FDBF5B9C0BDA009A3F16F 629F908E42D780B467147F7BC68398619DC18C3E20D4E4916E04 7B282

II. The stage of choosing the primitive polynomial equation / in step 3 in the algorithm

Table3. Complexity in (Hash-Qr) algorithm base on primitive polynomial

message	The initial val (1D)	Output Hash 128 HEXA
Zainab ali	$x^{12} + x^7$ $+ x^4 + x^3$ $+ 1$ And $x^2 + x^1 + 1$	6589A2AB4BCB0779FB7364870DFCB68F8A187B45D6654B30B759 1AAB16C3A7EBCD4B55F5598886D1B4C099F61DD7C9E73DF9174 1690DE626762DC61DD6128ED8BD40B9F387AAEB32365863EC165 9A058C6134C2842CF8E9316ECEC8418AEFB0CF26DA59B4114159 1219723521A43C960EA4EB64BFABDD8CE83780AB61CA01EE0
Zainab ali	$x^{15} + x^{13}$ $+ x^{11} + x^9$ $+ x^5 + x^3$ $+ x^2 + 1$	8C9CDA48E279859FD3F47A3F3D34972E42900F59A96095478E7AE DB0FFC4EF723D7AA4A0F2B98EB3F62A68F59505FB23244E4E9E BD29D6D860DDC8B24CABC181CBA6A262CDEB7870E62AF39F8 30A4A26CDC3B275B7CBE93416A5AB825377C5007709BA8B2ADA C1E941E3A6FEE5E51A44B6B4797A8F2C0BDFC08B3FA287C15D 50
Zainab ali	$x^{13} + x^4$ $+ x^3 + x$ $+ 1$ And $x^5 + x^2 + 1$	F087031EB9753B0589E3E4C390438721AD60FF05E726C0DBCBA5 3EFF80A7BA271CB46390E6B073DFB541E66BAEE0EB82F5DFBF7 F69514A9CD4C3095D4B40A077F438D35D4B6F25495896C82F8EA3 900B9E13685DD464F1BFEEF6C10820484F51D14651E74B5E8D654 4984BF03063137AD44EB6DC7198C4FAB57D1EB32444C529
Zainab ali	$x^8 + x^6$ $+ x^5 + x$ $+ 1$	91F43C0C5CBBFC03F1EA585A9CEFF861A6F3BFA0EFB3A9BBE F373ED28B1C38353408EC883B010FA643260244826BA3E784EDB1 73031F76B8071E02737D7F84165A4F195E02A8D7C96C7F534FD554

	And $x^{11} + x^2 + 1$	ADB60D772B641899407637F7A632C4B9D79009A778E755A2F607C7BCE4F29B3F9039CF773F2B32A01E4E9E0F0E30A49B346E
Zainab ali	$x^8 + x^6 + x^5 + x + 1$ And $x^{10} + x^3 + 1$	35D20C702F34F97DCEE06308326589E57B7BB237D46A8D439D7BEBE1673627DACA839A4C7B96E243C00ECACBC3D439F47C2A12A0B08402790CA7117C842724324E2D122ACE303D89558B8FA7251052D9E6E2AF56BE90A164667F7B384C94ECD65DB7032EF366819DD962FC1A5591F99C620ED76FB5AF9ECECF2A767F71DDFE02B

- **Collision resistance:** It is not possible to generate two different series for the same output, or generate one output for more than one input at a time. About 1000 hashes were generated using the proposed algorithm and it did not result in any collision.
- **Input and Output Size:** Any data size can be used as input while the output length is fixed

5.1. Statistical analysis of experimental results

Statistical analysis was applied to find the similarity between the inputs and outputs of the proposed algorithm. We used the Jacquard similarity coefficient, which measures the similarity and difference by finding the ratio of the intersection over the union as it is used for binary data.

$$J(A, B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cup B|}$$

- A= input message (binary)
- B= message Digest (binary)
- TEST 1:-

A= input message (zainab) made an expansion to 1024 bits
 B= message Digest output from (Chaos Buffer Hash) 1024 bits

Table 4. Jaccard Similarity and Differently Measure/Test1

Chaos Buffer Hah		
Message	Jaccard Similarity coefficient	Jaccard differently coefficient
Zainab	0.178	0.822

- TEST 2:-

A= input message (abdallah) made an expansion to 1024 bits
 B= message Digest output from (Chaos Buffer Hash) 1024 bits

Table 5. Jaccard Similarity and Differently Measure/Test1

Chaos Buffer Hah		
Message	Jaccard Similarity coefficient	Jaccard differently coefficient
abdallah	0.139	0.861

- TEST 3:-

A= input message (noor364583) made expansion to 1024 bits
 B= message Digest output from (Chaos Buffer Hash) 1024 bits

Table 6. Jaccard Similarity and Differently Measure/Test1

Chaos Buffer Hah		
------------------	--	--

Message	Jaccard Similarity coefficient	Jaccard differently coefficient
noor364583	0.1343	0.8657

➤ TEST 4:-

A= input message (السلام عليكم) made expansion to 1024 bits

B= message Digest output from (Chaos Buffer Hash) 1024 bits

Table 7. Jaccard Similarity and Differently Measure/Test1

Chaos Buffer Hah		
Message	Jaccard Similarity coefficient	Jaccard differently coefficient
السلام عليكم	0.1223	0.8777

➤ TEST 5:-

A= input message (12ur84ndlf0r) made expansion to 1024 bits

B= message Digest output from (Chaos Buffer Hash) 1024 bits

Table 8. Jaccard Similarity and Differently Measure/Test1

Chaos Buffer Hah		
Message	Jaccard Similarity coefficient	Jaccard differently coefficient
12ur84ndlf0r	0.1873	0.8657

The first test recorded a percentage of similarity and difference with a value 0.178 and 0.822.
 The first test recorded a percentage of similarity and difference with a value 0.139 and 0.861.
 The first test recorded a percentage of similarity and difference with a value 0.1343 and 0.8657.
 The first test recorded a percentage of similarity and difference with a value 0.1223 and 0.8777.
 The first test recorded a percentage of similarity and difference with a value 0.1873 and 0.8657.

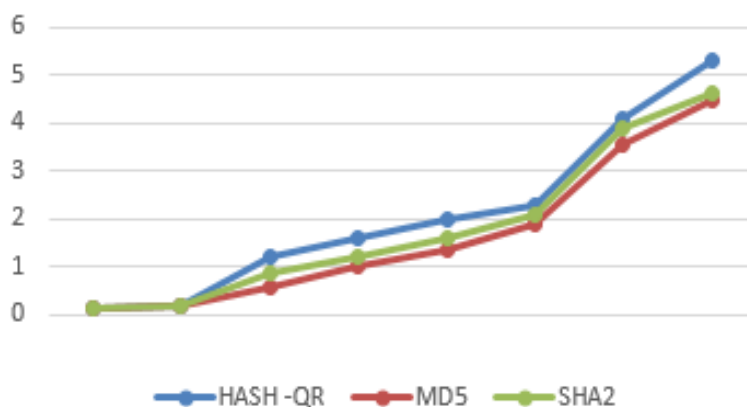


Figure 3. Comparison time between MD5, SHA2, and HASH-QR

Note in Figure No. 3 a comparison of the execution time of the algorithms, both hash, MD5, and propose an algorithm (HASH –QR). The execution time of the new algorithm (HASH-QR) does not exceed the time executed of MD5 and SHA2, except with a very small increase. The proposed algorithm (HASH –QR) has proven its speed despite its multiple operations.

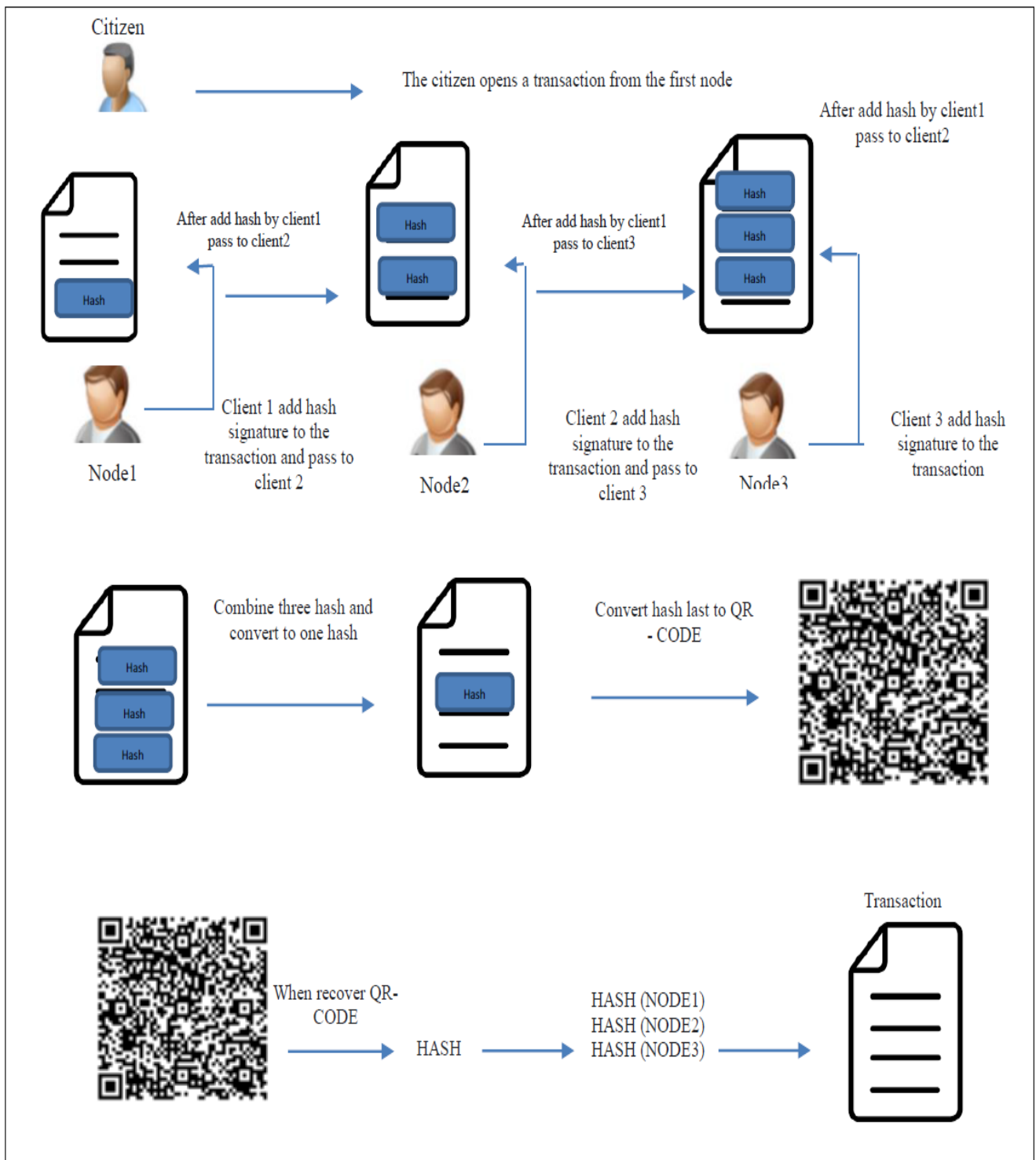







Figure 4. Comparison Time Between Md5, Sha2, And Hash-Qr

Figure 4 shows the mechanism of the proposed work, where three hash are generated from citizen data with employee data (Node) to obtain a common signature for all parties. It is then converted to a QR code to obtain a single encrypted signature.

It is possible to decode the QR code and obtain the complete data and signatures on the need to retrieve the data. Where the correspondence between the nodes is saved in all employee servers with the information of the complete transaction, in addition to that any movement in the system will generate a hash for a node.

Thus, the data will be retrieved through decoding the QR and it will be called through the node that was used to make a QR recovery.

Table 9. Samples experimental results that hash value with Qr-Code (Hash - Qr)

Information transaction	HASH (NODE1)	HASH (NODE2)	HASH (NODE3)	Combine hash1,hash2 and hash3	QR-CODE
IN:453456789 N:zainab ali kamal FC:54678ghjimo SC:5fscghjokl; THC:752sfghjkkoo	0C5E547FFD812108F14055B0 3F867940C752B3803C0581D3 0A772D47B655DC1CEBDD52 0C0C96E0D9C8B5D77AB769 9AADFB3D6E6A1C1C997F37 040CD1815D2123CDEE5CF8 0442137A4546452BCA4242 61B374C106A4F0BC8834933 F73697A14BF9DA3CE0B6F8 822A02CE0D80156F8D796EA 019F4F439BBF6A13F6A456A 8CA0F7	1B37AA2511C9059F732C9 BD11B1802D47CC57F4D82 2C4E4E92D8E024030E648F B43ECF9CED4D759EA7091 504182BAAC3ABF4F92013 F8DFF1C8814E0D725314B A9878AC109B377848B61FE 24C1942CD23E0B26E93055 913BE30B5145637FF459424 4630CA739379810914B55E B5778842748015A596D5A F81730A535BE431FC8	343E0C2C0F0628837B3C5908 830A054D9F762C22B5C28BC 5ABF499A622CD1D0595FEC 737F8912A009154298A494FC CAE9C3BE1724CE3FED24CE 20D0F247497EA312FF8A72C 5A54C9B286633E1739729D4 6482E5CF04BBCC7D0937854 E68C5BAB41120549C183E2E A9CE74B205D26E4AB6093D 82B5C900D3A192AB657B0E AC29	2357f276e34e0c14f9509769 a7947ed924e1e0ef0beb4458 335b9ae3d796a596ca1d5aa7 194bf47fee8ebf4e60dfc0cc f276384307b85cb3c8ec3d7 7aa27364b9084fb32f3fbb0c de52d44957e2c2e1a066a01 2a3bacef510244002165698 d2c7e5973c585a21d4cc6ca5c a6b716fe1252e189de1dd179 d6415afc11316	
IN:56321234332 N:alaa talib hasan FC:65rfghu8u SC:hgrfrim886 THC:ftfghjgh	B985330C4DCD141FB858B80 963A315B2CDECC684DD817 FF3B94D083BB2A9C0E0C34 AED8CCF058D6DA6045895F C54623960387B0787194F0F A8D759C8AC51C3D6F8062 B9C31FEE6A7C4EDEA3CD6 C6372FD1F78CE37A4B267D7 2ABC60B94DA43C82DBE881 FEA58EF5112E6E87CFD0E5 EBC968DC18BD45B3C74E43 47A7B42EAFB	1C35DA5B973D3DC652B9D9 7B7368169F192303E70146BC C4C840509FE25118D5A3693 C243F1F6F6F1163E557E9087 A3AA2FBA437F478F1A3106 5544770295926E1CC81034FD 5B9993A2DF6C35984D55151 4FF54B53E8280D4AC19EC37 4DB13EA892F899B350CF012 A1BCFC87FC6BB34F97205 15349D5C6FCCFE8F3462D31 0C9	87E23E2CAB97D9670E426AF B6086BA225673392AE9C70D 55D9CD11AE625AB85A92A5 00BD28C5E0B0441932101E1 88BBF6A6B8B0B2E276CC33 E44EA6CF4D54C5945E851E4 3A7E30667E3433FEF2FBE5 EFF28B62EE3BC289EA050C 5F43E8AEA9AB08C8BC1E6 6F5835A22058971F34067842 B7787AA6EC40559AB67F27 6443109	2252d77b7167f0bee4a30b89 704db90f82bcfe493500ce62a 8c0490a32a260633286d115d 8d402b2f37e8fd20b4493bb5e 4ea88ca22e09904daccb704 5044bc72cd6cce99a7279fa 0a58168a7dad3881b6b4e953 2e4bb597e3f0f141c52300ea0 afd2cc89f0c8528e42871c0f b320753f0ae19a54706e1b1 dcbc6fd5cb3b	
IN:646886545790 N:ali abed toama FC:bfghfjhkl SC:bftrhjk THC:grfghjgh	126E23D7F7A196B08BA6AD 7A21DAF9C7C990547985802 15CC9247E4D9A29AFC91663 984AE73AE19D26CD2B411B ABC578257EDD00F1F1DCE6 15C9A5A468BCCEDAE87F 6AF34EA3D05836FAD8D5F4 5A86E1306138C151505335D4 C877E28775456070BB47F518 E803977DAC8D8C3D910816E 62D4B05CE2FC30C716B214C 178D98E6	247585F48DB70D45FC9CA5E C6116E15B1D087B9D2156F0 711518CD6305AA954FF3FD6 E06827FEE4CBEAA2AEF284 EF8101DBF875CB83916C8FB 3B865F0CF8067C60399575E2 879CF79B3A21144377DF0751 45D3DC71428B6CFCB46A1B 0A68FB2540E819071A445863 46228A8306C604076D76DB DD1286D8C2D10AC504A3F9 60F	7C97E672D82A7A1AD4FF35 5434879B5F3F9220AF331960 AE18FA53903B730463321B6 A908EA845BC2819073929892 43C908904FB2E045EFDFC86 F1CC305C97FE0D41941CD4 EBB364D94A402CC8C1113D 0FD815123F25DA030F3B734 C808C1E75B279AB818E944 CACF97FF23C07137B8F5B1 DCEDA82279BF82FC0031097 58FA2	4a8c4051a23ce1ef90c53dc274 4b8c3eb0a0f4b97cfb183c4c6 e0bea4f03ee5d7859dcbed44 6db07e06971a6c1954aa6858 767ce94d31274d563c47185f5 87fff7e602861296c11fccb5a0f a66544d9b54252672545caec7 de29a293be941cc437fe33239c 90fe6fb82c9d26fe654fa55b 726e73fde878d2d45c7814b	
IN:678654333 N:ruqia firas salah FC:bfghj7igrf SC:bdgrf4ed THC:swv3edfityjo	59AE51F1E5E6D6B7967D15B 5E37AADE3505264357994556 B72BCEFA3A72D8223E10F4 F7B2D3728A25AC2BD25DC6 EC0480A03830A0BEFF70C70 B4A2B9D8B9253B205C291F0 5B5B1FA4391184C0955FE6C FCD5CAEA915C98E8B780E6 302F777EDCF866E424C166D B32529D7462B0C556FE5794 AC6A24A8351EFA35D5EE1F FB47E	3D8BB850E6A247FC9ED310 2C3D388A0BA4BE183A0F08 C0E40B64AB8F1C82D3BB56 9A1E06BCFE48D7F29EAAD9A C40975EF837FC1FD9EAD9A 414EB6C6303AF86C062C24B 1C243CA0DB6697A469C04E 1D5E0649D65F333F7F6E693 641375F04947F3B7A518F2D6 CF2A82FFA6F1790A7F469FE 3FA99F70377B10F6C733715F 8C9920	C034A330A388ED7712C8779 18159216B48632E833A23857 3C4D345F79BDC3162E37FB7 EB50A9BF8519ABB4A7EFA F46472C03BB0BC064BF55CA D54587EEFA84CCDB3BEF ABDFDA08B525A27EE72CF ABF569A43115285606C1A15 4BD8E191F9403CE1D0C58A 7818487E25EBCB43ACE7569 BD55CE3F766DD886655953 DEA48B9BCB	a4114a91a0cc7c3c1a667208 5f1b0683bc8f528c4cbf10fcb d0b0142207360fa54eae696c 160dff06ac8a39dfc8850a5 7f9fc5526d218f563c47f0da bcdfl d74377699a5b490f47 c037214e94da020b6be4b4703 8b9ccbdf7fe618aa922cc7 021941261e4588cd0368c85f 41d7e182d66a41020c97c3d3 dfl1af8b695	
IN:8753456 N:yousif basim jasm FC:zqaqwdrf78 SC:vdgr90jgf THC:ljohf7689	2F106E5D21B889E837F1C41 2C46E0A4BD7F6F3A57FAB4 E1E6769BB56729EA6140B12 A91ECB97F09E706AB254B7 E8844AA3BC6056A46659600 2314933F2289EABFFB57C90 50BCCF0A1DCDE5C16421F9 621321A31FA521E87298F74E ACB12B495A46506846CEAE F58288E5E773B26DD68F7BB 03CF99C17EA16358EB3034 C6B83C	5E3B137074A562DF407DAD 9EE32FE7993711C247E0BD5 E06E5D39446FB02D49BFE1F 49496103F72B2720E54A19AF ED4D40D9BA4A7FA0138193 C0FCA1A0DB73583B46042D 5E38FFCC74D73A3B3FFC7 774181E89CE45441EE9095C1 C1D91A50FFD4CD1A415034D E90094D5E9B110CE19FBE18 7D278FE699B3B0CD2C952C 6898AC6	2A5289AE5B38DDB0546D71 BF3A14033FCB5900ED489F5 6CC794B25EF20F77295A42 C127C7591E7A9D558E50B68 8D399EDCB29FCDAC19CE9 73209835E917D302EB59797F 890C7F18D176B7E4734BB06 E6FC61011DA514D3E2C9A6 EB1F1E832ABB2E01955CA 32EE1A127E1881CA2086D53 C896B60ADD8F1BB8E6FB4 E2A2D8656	5b79f4830e25368423e1183 31d55eed2bbe310f878946 44bf10affa69b856a6a4e217 06dcd19cfca1fd9418cfba9 e0eae48e00107d601e2d12d a7bbe43ef12faa01528a533f ee0b82186a4958e7b3d665 b929b24e4a2248fe1dc9949 2b0cb1afcd691403263bd1 7ef4abe01c719c9f878326d7 55a81d76cd92cd862b4ac	

The presented system is feasibly enhanced more by IoT , e-government, cloud computing and Arduino tools as future trends of this study [28-30].

6. Conclusion

This work presents a new method for data retrieval in a more secure manner, which depends on the generation of a QR based on the signatures that are generated depending on a new hashing algorithm after the transaction is proposed by the participating parties. All correspondence between the nodes will be stored in the node's servers and all signatures will be saved. After a decision is made on the transaction, it will be given a QR for contract signatures. Recovery of the contract is made based on this QR, it will retrieve all correspondence with the transaction information so we have provided a new way to retrieve the data. Where a new method was used to generate the hash. This method has proven its efficiency by conducting many theoretical and practical tests.

References

- [1] W. J. Luther, "Bitcoin and the future of digital payments," *The Independent Review*, vol. 20, no. 3, pp. 397-404, 2016.
- [2] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European conference on technology enhanced learning*, 2016, pp. 490-496: Springer.
- [3] V. Morabito, "Business innovation through blockchain," *Cham: Springer International Publishing*, 2017.
- [4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.
- [5] S. Ølnes, "Beyond bitcoin enabling smart government using blockchain technology," in *International conference on electronic government*, 2016, pp. 253-264: Springer.
- [6] D. Allesie, M. Sobolewski, L. Vaccari, and F. Pignatelli, "Blockchain for digital government," *Luxembourg: Publications Office of the European Union*, 2019.
- [7] C. Brunner, F. Knirsch, and D. Engel, "SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain," in *ICISSP*, 2019, pp. 15-25.
- [8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2084-2123, 2016.
- [9] S. M. M. Najeeb, H. T. Salim, and S. M. J. T. Ali, "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," vol. 19, no. 1, pp. 285-292, 2021.
- [10] 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.
- [11] H. T. ALRikabi, H. Tuama, "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.
- [12] G. O. Karame and E. Androulaki, *Bitcoin and blockchain security*. Artech House, 2016.
- [13] M. A. Roa'a, I. A. Aljazeera, S. K. Al_Dulaimi, and H. Alrikabi, "Generation of High Dynamic Range for Enhancing the Panorama Environment," *Bulletin of Electrical Engineering*, vol. 10, no. 1, 2021.
- [14] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*, 2017, pp. 464-467: IEEE.
- [15] E. Q. Ahmed, I. A. Aljazeera, A. F. Al-zubidi, and H. T. S. ALRikabi, "Design and implementation control system for a self-balancing robot based on internet of things by using Arduino microcontroller," *Periodicals of Engineering Natural Sciences*, vol. 9, no. 3, pp. 409-417, 2021.
- [16] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure e-document," *IEEE Access* vol. 8, pp. 80290-80304, 2020.
- [17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 2017, pp. 618-623: IEEE.
- [18] H. T. Salim, and N. A. Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 13, pp. 4-15, 2021.

-
- [19] H. S. Abdulah, M. A. H. Al-Rawi, and D. N. Hammod, "Message Authentication Using New Hash Function," *Al-Nahrain Journal of Science*, vol. 19, no. 3, pp. 148-153, 2016.
- [20] A. Ali, M. Rahouti, S. Latif, S. Kanhere, J. Singh, U. Janjua, A. N. Mian, J. Qadir, and J. Crowcroft, "Blockchain and the future of the internet: A comprehensive review," *arXiv preprint arXiv:00733*, 2019.
- [21] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "Blockchain-based smart contracts-applications and challenges," *arXiv preprint arXiv:04699*, 2018.
- [22] H. T. S. Al-Rikabi, *Enhancement of the MIMO-OFDM Technologies*. California State University, Fullerton, 2013.
- [23] L. Ante, "Smart contracts on the blockchain—a bibliometric analysis and review," *Telematics Informatics*, p. 101519, 2020.
- [24] Y. Xu, H.-Y. Chong, and M. Chi, "A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective," *Advances in Civil Engineering*, vol. 2021, 2021.
- [25] 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.
- [26] F. Lautert, D. F. Pigatto, and L. Gomes, "A fog architecture for privacy-preserving data provenance using blockchains," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, 2020, pp. 1-6: IEEE.
- [27] A. F. Kadhim and Z. A. Kamal, "Dynamic S-BOX base on primitive polynomial and chaos theory," in *2018 International Conference on Engineering Technology and their Applications (IICETA)*, 2018, pp. 7-12: IEEE.
- [28] A.A.H. Mohamad, Y. S. Mezaal, S. F. Abdulkareem, "Computerized power transformer monitoring based on internet of things," *International Journal of Engineering & Technology* 7, no. 4, pp.2773-2778, 2018.
- [29] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, and S. F. Abdulkareem. "Iraqi e-government and cloud computing development based on unified citizen identification." *Periodicals of Engineering and Natural Sciences*, vol.7, no. 4, pp.1776-1793, 2019.
- [30] Z.K. Hussein, H.J. Hadi, M.R. Abdul-Mutaleb, Y.S. Mezaal, "Low cost smart weather station using Arduino and ZigBee." *Telkomnika* , vol.18, no. 1, pp.282-288, 2020.