A Novel Model for Securing Seals using Blockchain and Digital Signature based on QR Codes

May Wezza
Mansoura University
M. M. El-Gayar (✉ mostafa_elgayar@mans.edu.eg)
Mansoura University
Ahmed AboElfetoh
Mansoura University

Research Article

Keywords: Stamp Seal Imprint, Digital Signature, QR code, Blockchain, Smart Securing Model

Posted Date: September 8th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2031413/v1

A Novel Model for Securing Seals using Blockchain and Digital Signature based on QR Codes

May Wezza[1], M. M. El-Gayar *[2,3] [0000000246441835], Ahmed Abo Elfetoh[4]

[1]*Department of Information Technology, Faculty of Computers and Information, Mansoura University, 35516, Mansoura, Egypt*
[2]*Department of Information Technology, Faculty of Computers and Information, Mansoura University, 35516, Mansoura, Egypt*
[3]*Faculty of Computer Science and Engineering, New Mansoura University, New Mansoura, Egypt*
[4]*Department of Information Systems, Faculty of Computers and Information, Mansoura University, 35516, Mansoura, Egypt*

**Corresponding Author: M. M. El-Gayar, Email:* mostafa_elgayar@mans.edu.eg

Abstract

Every person in the world needs documents that prove their identity, graduation from the university, residence, marriage, and other essential records that must be safely handled. The credibility of the documents depends on the stamp seal imprints found in them belonging to the government entity, the source of the credibility. But recently, with the rapid development of technology, the number of forged documents and forged stamp seals imprints has increased tremendously, which has led to significant security and social problems. Most of the world's governments depend on securing documents by securing stamp seal imprints through using Ultra Violets inks and issuing them through a centralized environment, which contains many challenges and problems. Central repositories may have security issues such as a single point of failure challenge, data unavailability due to central system failures, or a Denial of Service (DoS) attack. Therefore, this paper will present a proposal that solves the challenges in electronic systems (complete digitalization) and paper systems (partial digitalization). This manuscript proposes a smart securing model to secure stamp seal imprints by encrypting data with stamp seal image of the seal and storing it as a block through the decentralized Blockchain platform. After that, a quick response code (QR) is created to access that block quickly and securely. Also, the stamp seal's hash image and the details of the stamp seal's data source in the blockchain provide a shared, immutable, and transparent history of the stamp seals without relying on any third party. After several experiments, the results proved an accuracy and security rate of stamp seals and documents that reached 98%, with a high retrieval speed. Thus, a safe, fast, and non-changeable environment was provided to retrieve necessary information and ensure its authenticity.

Keywords: Stamp Seal Imprint, Digital Signature, QR code, Blockchain, Smart Securing Model.

1. Introduction

In the current era, due to the rapid development in the technological and digital field, many countries have turned to the complete digital environment of smart cities and dispense with the paper environment because of the environmental and health problems it contains and high cost. However, the comprehensive or almost complete digital environment includes many issues, the most important of which is how to secure it in an accessible manner without hacking. Every day worldwide, many fake paper or electronic documents are discovered. The proliferation of tools such as highly advanced technology software, printers, and scanners that professional counterfeiters work on has made it difficult for the average employee in government and private sectors to detect forged documents. We can summarize some of the challenges that we will overcome in this article in the following points [1–4]:

- Some methods of securing documents or stamp seals may need a complete electronic system and may not work or perform the task successfully in paper-based systems.

- Most of the application of security and protection methods is through a centralized environment, which contains many problems such as a single point of failure, data availability due to some losses, and vulnerability to attacks.

- The difficulty of discovering the forgery of stamp seals and the violation of the credibility of many essential documents by many government agencies is due to having a daily forgery expert.

- To detect forgery documents or stamp seals may take days or even months in some cases, which leads to the complete disruption of the institution.

Table I – Some of important terminologies.

Terminology	Dentition
Stamp seal mold	Copper or plastic cereal mold which engraved to form definite shape or design. In the case of creating governmental stamp seal mold, special securing software is used for engraving the state problem, which represents the country symbol.
Stamp seal imprints	It is the imprint which formed when using the stamp seal mold on paper mechanically.
Stamp seal printout image	It is the image of the stamp seal which is formed by printing the stamp seal from computer on secured paper. In this case we have the stamp seal as printout image in partially digitalized system.
Stamp seal electronic image	It is an image of the stamp seal on complete digitalized electronic system without printout it.
Blockchain Platform	Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

As shown in fig.1, most countries all over the world are still put their stamp seals imprint mechanically. To create an Auto-ink genuine stamp seal mold, our government in Egypt uses a laser engraving technique operated by special security software to engrave the mold. Also, in partial digitalization in many countries, they use the stamp seal printout as an image formed by printing on security paper with QR Code. Although the stamp seal printout is genuine not forged, it is the printout from the most commonly used printer which are laser or Inkjet. The term "security paper" refers to paper used in security printing that has Security features that identify or authenticate a document as original, such as security printing offset, watermarks, security fibers, UV reactive ink, Optical variable Device i.e., kinegram and hologram, microprint and many other security features. Security paper can be used in Currency, passport, ID, Driving license, academic certificates, and any official documents. The importance of using the security paper is to be difficult to counterfeit and to facilitate fraud detection. There are minimum requirements each country should follow in securing their documents. But, a normal person or un-specialized employee can't detect forgery of the official documents in most cases, it needs a forensic expert.

- Security printing offset: This type represents the base of printing in all official documents, including passports, ID, Driving licenses, and Currency.

- Watermark: Watermark is created during the stage of paper pulping. The difference in fiber thickness forms many types and shapes of the watermark. Watermark is very difficult to be counterfeited as it is produced during the primary stage of paper manufacturing.

- Security fibers: Very thin fibers are embedded randomly during paper manufacturing. It can be red, blue, green, or any other color. It can be visible with normal light or invisible with normal light and appear under Ultraviolet light. Security fibers are very difficult to be counterfeited as it is produced during the primary stage of paper manufacturing.

- UV reactive ink: It is the ink that contains in its ingredients one component that reacts with UV. UV reactive ink can be invisible under normal light and visible under UV light. Another type can be visible under normal light and change its color under UV color, i.e., the written ink is under normal light black and changes when exposed to UV light into red color.

- Microprinting: Printed text is very small and needs a magnification lens or microscope to appear clearly. It is seen as lines without magnification and can be read as text under magnification.

- Optical Variable Device (OVD): The most used types of OVD as security features are Hologram and Kinegram. A hologram is an anti-counterfeiting feature added to most documents and Banknotes. It is used to refract light due to nanostructures that refract light by tilting the document or Banknotes. When light fall on a flat surface, it appears in a 3D effect, so the light is changed to a lot of different light, or the shape seems to be moved to form another shape.

The forgers attempt to create fake stamp seal imprints using various forgery techniques:

- The first type involves forgers trying to imitate real stamp seal mold by making fake versions by engraving them with special chemicals or by laser engraving. To examine the suspected stamp seal imprint in this situation, the forensic examiner needs a reference of a real stamp seal imprint.

- The second type by producing counterfeit stamp seal imprints by printing. Forgers use a lot of printing techniques to imitate genuine stamp seal imprints i.e., Laser printing, Inkjet printing, and screen printing. The three printing techniques create fake stamp seal printout that should be examined and detected only using a magnification lens or microscopes.

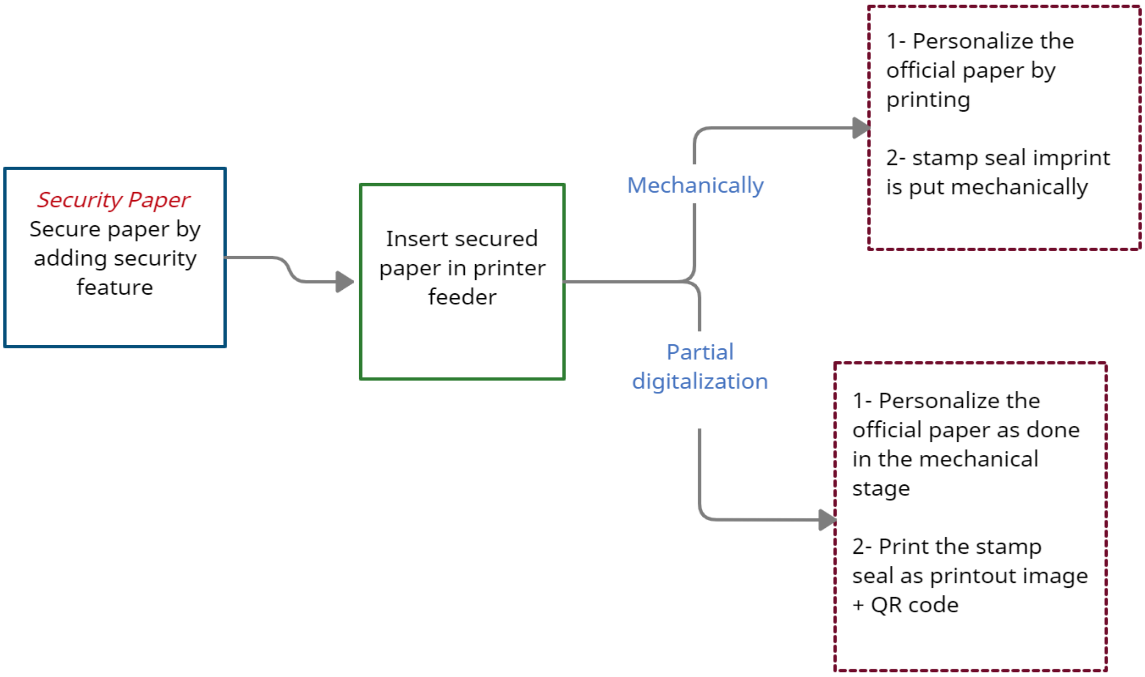

Security Paper
Secure paper by adding security feature
Insert secured paper in printer feeder
Mechanically
Partial digitalization
1- Personalize the official paper by printing
2- stamp seal imprint is put mechanically
1- Personalize the official paper as done in the mechanical stage
2- Print the stamp seal as printout image + QR code

Figure 1. Stamp seal imprints and printout.

A consensus mechanism refers to a protocol responsible for ensuring that all the participants in the blockchain network are following the agreed rules to confirm blocks to be recorded on the chain [5,6]. Blockchain does not need a centralized authority to operate. The blockchain network, rather, requires its participants to verify and authenticate the activities that occur in it. The entire process is done on a consensus mechanism basis, and it makes the blockchain a trustless, secure, and reliable technology for digital transactions. There are many consensus mechanisms of different principles that enable the network participants to follow those rules. Fig. 2. shows the taxonomy of consensus algorithms.

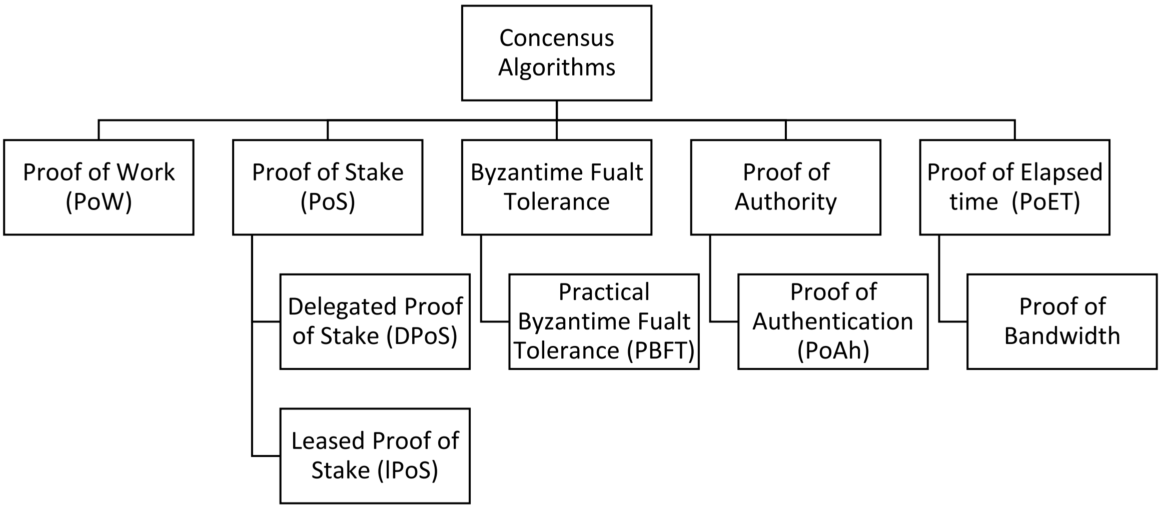

Concensus Algorithms
Proof of Work (PoW)
Proof of Stake (PoS)
Byzantime Fualt Tolerance
Proof of Authority
Proof of Elapsed time (PoET)
Delegated Proof of Stake (DPoS)
Leased Proof of Stake (lPoS)
Practical Byzantime Fualt Tolerance (PBFT)
Proof of Authentication (PoAh)
Proof of Bandwidth

Figure 2. The taxonomy of consensus algorithms [6].

To overcome these challenges, document verification should be a mandatory checking step for both the paper document and the digital document to get around this problem. To achieve document authentication, the data must be stored to be impossible to change, hack or spoof. Also, the storage data must be decentralized, multiplexed, and distributed across an entire network of computer systems allowing all participants to operate the stored data or records. Document verification can be achieved optimally by applying Blockchain technology [1,7,8]. We can summarize some of the contributions in this article in the following points:

- We propose a smart securing model to secure documents, stamp seals and store them as a block through a decentralized Blockchain platform

- Encrypting the data of the stamp seals, such as the data of the concerned employee, the institution number, the date of issuance and other data, in addition to the stamp seal image in a digital signature way, due to the difficulty of obtaining or falsifying it.

- Generate a QR code to access encrypted information quickly and securely. After that, the authorized parties can remove the encryption and see the data. QR code allow us to perform a hybrid system for accessing electronic or paper-based system.

- The stamp seal image and the source details of the stamp seal data in the blockchain provide a shared, stable, and transparent history of the stamp seal without relying on any third party.

The rest of this manuscript is separated into five parts. Part II reviews some of the previous work related to our field. Part III represents the proposed framework and explains the different stages with the proposed algorithms. Part IV describes the experimental results of some test cases and the discussion section. Finally, Part V will provide conclusions and references.

2. Literature Review

In this section, we will review the various technologies and methods that have been used to share and secure documents. In addition, this part concentrates on the distinct styles used recently in many prestigious journals.

Singhal et al. [9] presented a technique to prevent the circulation of fraudulent degree certificates using a smartphone application and QR Code. Authors used digital signatures to encrypt data such as the holder's name, enrollment number, registration number, total marks achieved, and so on, which university officials will sign. A user must use a particular smartphone application to verify the digital signature by scanning the QR code.

Yermack [10] considered how Blockchain affects institutional investors, auditors, small shareholders, managers, and other participants in corporate governance. Authors presented the benefits of Blockchain, such as cheaper, better liquidity, more precise record-keeping, and ownership transparency may dramatically shift the power balance among these generations.

Sullivan et al. [11] conducted a performance analysis of the use of Blockchain in e-Residency can radically alter how identification information is managed and verified. The legal, policy and technological consequences of this development are examined in this study.

Pongnumkul et al. [12] conducted a performance analysis of the use of two prominent private blockchain technologies, Hyperledger Fabric and Ethereum. Hyperledger Fabric regularly beats Ethereum across all evaluation criteria, including execution time, latency, and throughput, according to the testing results, which are based on different numbers of transactions. Furthermore, both platforms are still not competitive with existing database systems in terms of performance in high-load circumstances.

Xu et al. [13] presented the educational certificate blockchain (ECBC) system. This system can operate with low latency and high throughput. This system effectively provides data on time and is suitable for the infrastructure of decentralized electronic systems. But it does not offer sufficient security for information in terms of authenticity.

Saha et al. [14] proposed a system that allows users to create digital signatures for documents and articles online, as well as interact without having to use any difficult methods. This system, rather than encrypting the entire text, creates signatures based on basic information contained in any document. But this system works on a central network that does not provide a fast environment for the availability of information, as it is considered a single point of failure and can be easily penetrated.

Nguyen et al. [15] suggested a method for issuing immutable digital certificates that use blockchain technology to overcome the current limitations of traditional certificate verification systems, such as being more trustworthy and independent of a central authority. The results show that their proposed system is an acceptable ICT-based e-government solution, especially in managing certificates and diplomas. But this proposed system does not provide the speed and ease necessary for the availability of data on time.

Cheng et al. [16] proposed a system that can handle all kinds of official documents through Blockchain technologies to provide a secure environment that cannot be changed or tampered. However, this system does not provide sufficient data confidentiality. Also, it cannot determine the source and reliability of the data.

Khan et al. [17] proposed an intelligent system for the Dubai e-Government Private Economy Department that integrates new technologies to use the blockchain to make Dubai a more innovative city. Dubai Smart Government has used blockchain technologies to make transactions more accessible and stable. But this system needs techniques to know the data source and detect its forgery.

Xu et al. [18] proposed an Electronic Certificate Catalog Sharing System (ECCS) that relies on the blockchain consortium to improve the efficiency and accessibility of e-government delivery service by implementing time and data immutability in the blockchain. According to the security analysis, ECCS can protect the privacy of certificates and electronic catalogs from unauthorized individuals. But the system needs to ensure data integrity and authentication of data sources.

Suma [19] described blockchain-based security and privacy mechanism that prevents the misuse and corruption of large amounts of court-generated data, security records, legislation, trade code, and other sources. Using Rivest, Shamir, and Adleman (RSA) method, the proposed solution ensures the reliability and credibility of data exchange over communication channels. However, this system does not provide easy access to data anytime and anywhere through a QR code.

Geneiatakis et al. [20] studied whether the e-government service can be decentralized using the blockchain. The authors propose a system that supports commodity exchanges across the European Union. The results indicate that the implemented system can meet the standards related to productivity and information availability. However, the system cannot detect counterfeiting or the reliability of the sources.

Bharadi et al. [21] introduced a blockchain-based system to create trust and integrate different subunits of local public service systems. The existing system used the Azure Blockchain Workbench to connect these modules and keep them in sync and confident.

Xie et al. [22] used blockchain technology and smart contract to build a decentralized certificate system. Some certificate management, issuance, authentication, and revocation functions were implemented using smart contracts. In addition, signer data, certificate prototype data, and certificate data were embedded in a smart contract, making it easy to query and validate certificates. However, this system does not maintain the confidentiality of the data.

He et al. [23] proposed an access control for sharing the data to avoid security issues over cloud. Authors used blockchain technology using attribute basis hierarchical scheme as access control scheme. However, this system does not maintain the confidentiality. Also, the authors did not say which blockchain platform was used.

Sun et al. [24] constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records. They used ciphertext policy attribute-based encryption system and IPFS storage environment, combined with blockchain technology.

Gao et al. [25] used blockchain technology to handle the problems in Notarial Office (NO). This system was built on top of the Hyperledger Fabric. Furthermore, they used smart contracts to substitute manual procedures, create additional ledgers to offload different sorts of transactions, and encrypt sensitive data as necessary.

Table II shows a comparison of the existing platforms of blockchain. Table III shows the summary of recent related works through several comparisons such as distributed data availability, performing a hybrid platform (support electronic and paper-based systems), performing data encryption to ensure data confidentiality and ensure data authenticity.

Table II- Comparison between different Blockchain platforms.

Platform	**availability**	**Popularity**	**Consensus algorithm**	**Pricing**	**Supported languages**	**Smart contracts**
Bitcoin	Public	High	PoW	Free per transaction	Script and C++	No
Ethereum	Public, permissioned	High	PoW and PoS	Ether for translation and computational service	Python, Go, C++, JavaScript	Yes
Hyberledeger-Fabric	Private, Permissioned	High	PBTF	Open-Source	Python, Golang, Java	Yes
Multichain	Private, Permissioned	Medium	PBTF	Free, Open-Source price	Python, C#, JS, PHP, Ruby	Yes
Quorum	Public, Permissioned	High	Raft, IBFT	Fees per transaction	Python, Go, C++, JavaScript	Yes
Lisk	Public, permissioned	Medium	DPoS	Fees per transaction	JavaScript	Yes
LiteCoin	Public	Low	Scrypt	Fees per transaction	C++	No
HDAC	Public, permissioned	Low	EPoW	Fees per transaction	Web Assembly	Yes
IOTA	Public, Permissioned	Low	PoW, TANGLE	not clear	Python, C, JavaScript	No

Table III- Summary of recent related works

Ref.	Support Distributed Data Availability	Support Hybrid Platform	Support Digital Signature	Support Data Authenticity
[9]	×	√	×	√
[10]	√	×	×	×
[11]	√	×	×	×
[12]	√	×	×	×
[13]	√	×	×	×
[14]	×	×	√	√
[15]	√	×	×	√
[16]	√	×	×	×
[17]	√	√	×	×
[18]	√	×	√	×
[19]	√	×	√	√
[20]	√	×	×	×
[21]	√	×	×	×
[22]	√	×	×	√
[23]	√	×	×	×
[25]	√	×	√	×

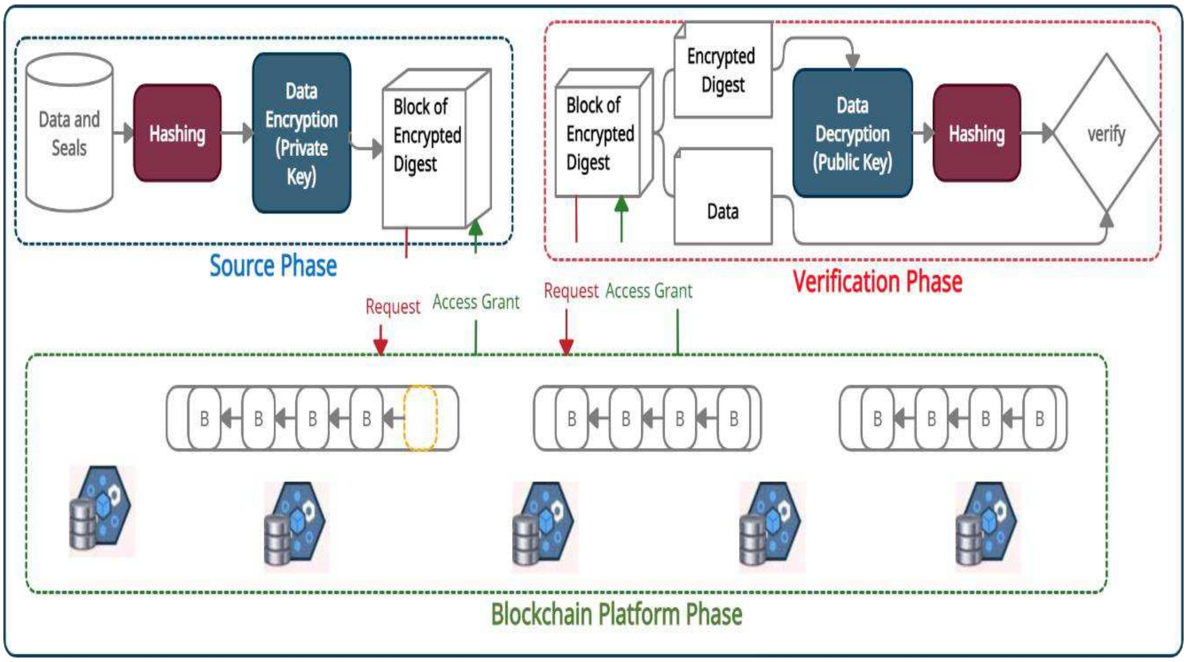

Data and Seals
Hashing
Data Encryption (Private Key)
Block of Encrypted Digest
Source Phase
Request
Access Grant
Block of Encrypted Digest
Encrypted Digest
Data
Data Decryption (Public Key)
Hashing
verify
Verification Phase
Request
Access Grant
B
Blockchain Platform Phase

Figure 3. General steps of the proposed model.

3. Proposed Model

In this section, a proposed model for securing the smart seal within important official papers will be reviewed. Fig.3 shows the general steps of the proposed model. The proposed model contains three primary stages. At the source phase, the organization's seal and the employee's data are encrypted using the organization's private key to output the encrypted digest. Also, an encrypted digest is converted into a QR code to be verified easily with paper-based systems. At the Blockchain platform phase, an encrypted digest as a transaction is formed into a block by the organization's node on the Ethereum open-source distributed network. Then, this block is linked to other transactions together in a network to make tampering difficult. After being granted access control to this blockchain block from the Blockchain platform in the verification phase, this block is divided into a hash digest and original data. The digest is decrypted using the organization's public key. At the same time, the actual data is hashed using the same hash function to produce the new digest. Then, the decrypted digest and the new digest are compared together. If the result of the comparison is true, then the block is authenticated and reliable.

3.1. Source Phase

At this phase, the seal or document source (the official organization responsible for creating the document or seal). As shown in fig.4, this phase begins with entering the data of the concerned employee (such as the employee's name, the job code, the organization code, ... etc.) to the hash function (i.e. SHA 256) for producing the hash value or the digest. After that, the digest is encrypted using the source's private key. Then, the encrypted digest is appended to the original data to produce the ledger block stored within the distributed network in the Blockchain platform.

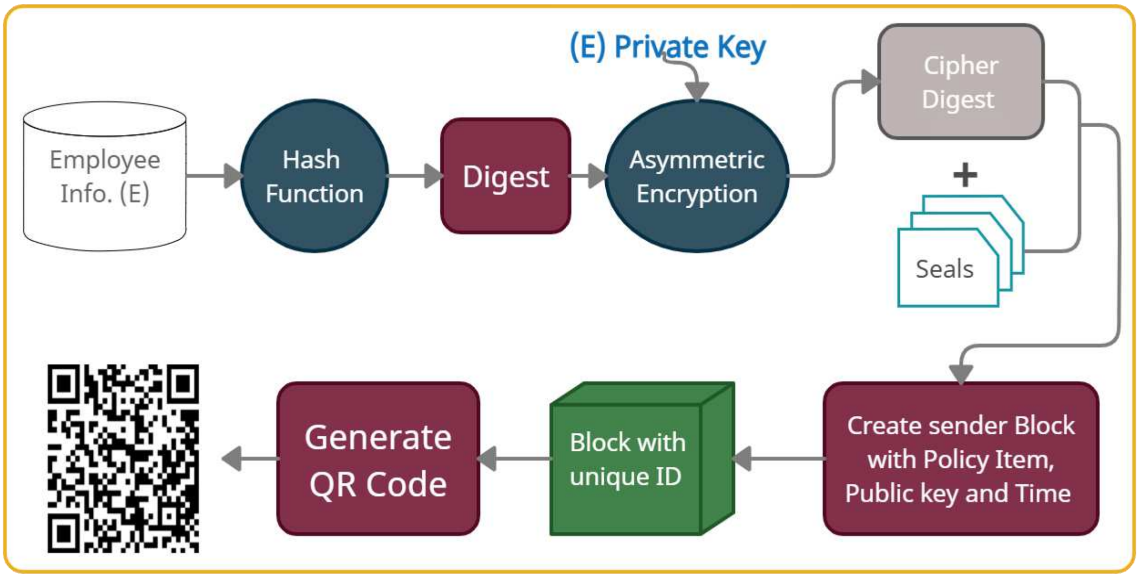


Figure 4. Block diagram of source phase.

Each block contains a set of essential data in its header such as the block ID (BID), the encrypted hash value (BKH), a timestamp, the source's public key (puk), the usage policy, and a previous block pointer as shown in fig.5. Block's header is implemented in two different types (request and response for granting access the Blockchain platform) using JavaScript Object Notation (JSON) format, as shown in fig.6. Finally, if the status of the block is approved to be stored within the Blockchain network, a QR code can be generated using the block's ID. The QR code can also be printed on the paper document inside the paper system.

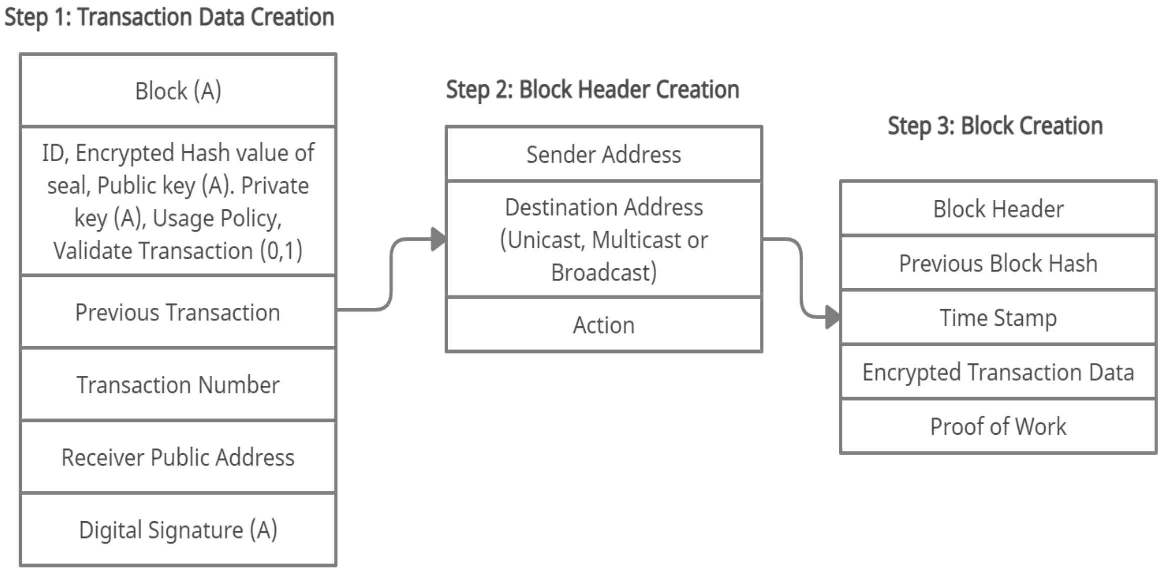
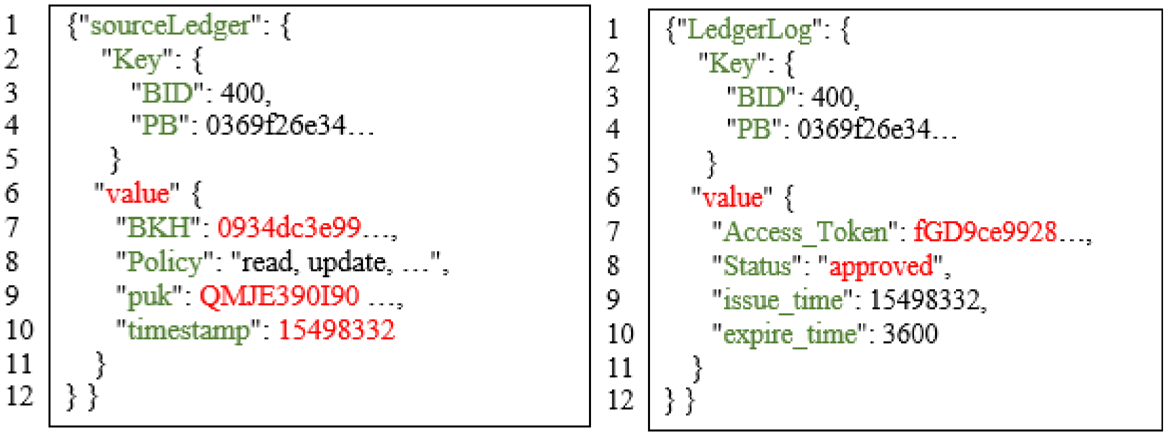

Step 1: Transaction Data Creation
Block (A)
ID, Encrypted Hash value of seal, Public key (A). Private key (A), Usage Policy, Validate Transaction (0,1)
Previous Transaction
Transaction Number
Receiver Public Address
Digital Signature (A)
Step 2: Block Header Creation
Sender Address
Destination Address (Unicast, Multicast or Broadcast)
Action
Step 3: Block Creation
Block Header
Previous Block Hash
Time Stamp
Encrypted Transaction Data
Proof of Work

Figure 5. Steps of Block Creation.



```
{"sourceLedger": {
   "Key": {
      "BID": 400,
      "PB": 0369f26e34…
   }
  "value" {
     "BKH": 0934dc3e99…,
     "Policy": "read, update, …",
     "puk": QMJE390I90 …,
     "timestamp": 15498332
   }
} }
```

(a)

```
{"LedgerLog": {
   "Key": {
      "BID": 400,
      "PB": 0369f26e34…
   }
  "value" {
     "Access_Token": fGD9ce9928…,
     "Status": "approved",
     "issue_time": 15498332,
     "expire_time": 3600
   }
} }
```

(b)

Figure 6. The content of different block headers in the Blockchain. (a) Content of the requested block header from ledger source to add new block into Blockchain platform based on a JSON format. (b) Content of the response block header from ledger log to source ledger based on a JSON format.

QR code is a two-dimensional barcode, and it has many benefits compared to other codes such as single dimension barcodes [26]. Also, it has a suitable mechanism for encrypting information. Furthermore, the QR code is fast, flexible, easy to read, and fault tolerant. The data capacity of the QR code varies relying on the data it maintains; it can carry up to 2953, 4296, or 7,089 symbols for binary/byte formats, alphanumeric or numeric, respectively. However, a classic one-dimensional barcode can maintain a maximum of only 20 digits. In fig.7 represents how binary image can be compressed and converted into QR code using Huffman-coding algorithm and XOR method.

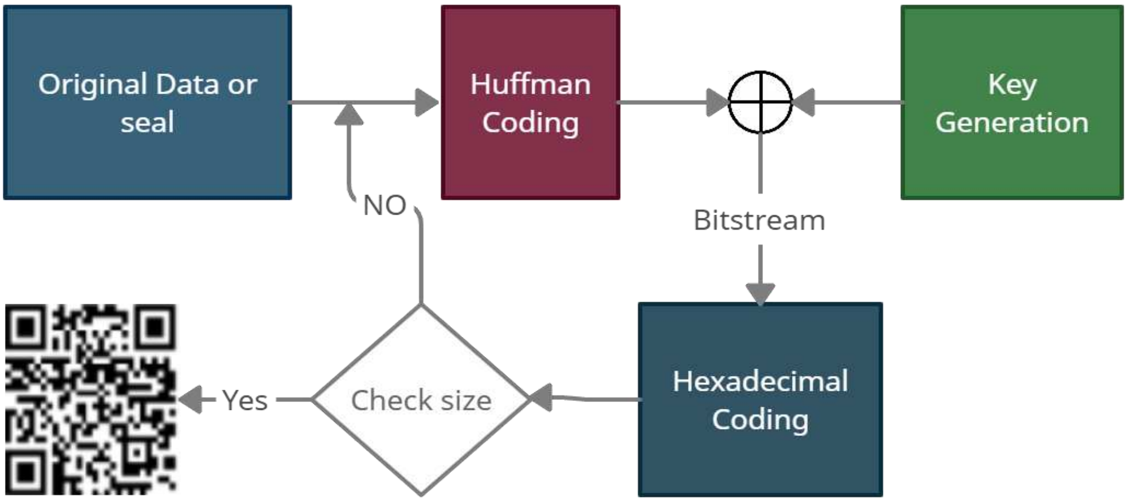


Figure 7. Generation of QR code.

3.2. *Blockchain Platform Phase*

The blockchain concept was proposed in 2008 as an alternative to the inconvenient central database by Satoshi Nakamoto. Blockchain technology links many blocks as a distributed ledger of successful transactions through many nodes so that it is difficult to counterfeit or manipulate them. This technology has been used in many fields, such as creating smart contracts, education, finance and linking patients' health records. The first block in the Blockchain platform is called Genesis Block. Then each block is connected to the group of blocks that belong to the same ledger as shown in fig.8. This technology was used because it provides decentralized transactions and proof of work [27,28].

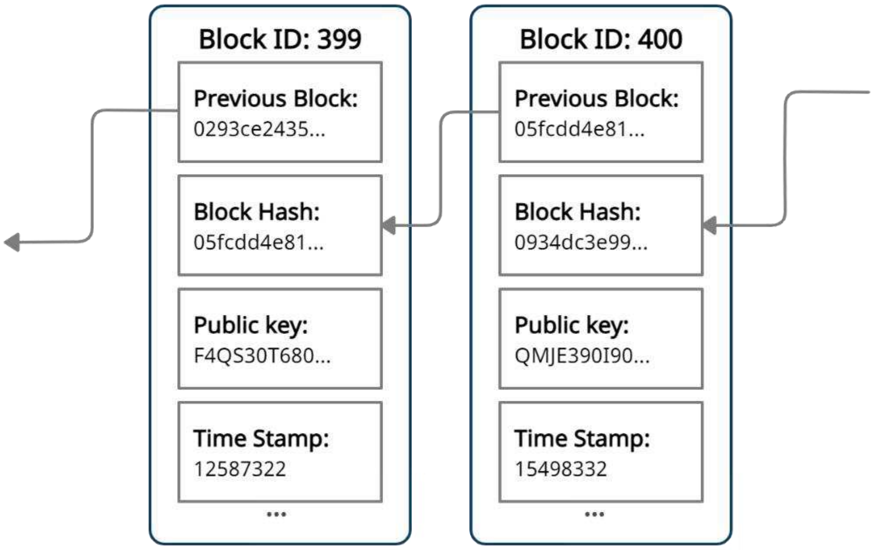


Figure 8. Two blocks are connected via previous block pointer.

In the previous stage, the inputs were the organization data with seals, and the outputs were a block or a group of blocks that contained the encrypted digest. But, this block needs approval to be appended in the Blockchain platform via the ledger's log. Therefore, the main role of this phase is to register the concerned block after performing the authentication process to verify its identity. So, algorithm 1 is used to determine each block's signature by ensuring that the encrypted digest encodes the original message with the secret key. To determine the identity of the source of information, we need three steps:

- Step 1: If the source chooses domain parameters $(p, q \text{ and } g)$ where p and q are N bits prime numbers. Then, the source can determine the private (prk_{BID}) and public (puk_{BID}) keys for the concerned Block ID using RSA or Digital Signature Algorithm (DSA). Then, the extracted puk_{BID} is compared with the public key provided during the request.
- Step 2: applying the proposed algorithm 1 that accepts puk_{BID}, prk_{BID} and original data (M_{BID}) as input. Then, it produces signature (S_{BID}) by singing equation 1 as output. Hv is hash value. k is random value form 1 to q-1.

$$S_{BID} = (puk_{BID}, prk_{BID})Sign(Hv_{BID}, k, M_{BID}) \tag{1}$$

- Step 3: applying the proposed algorithm 2 that takes $(sign_{BID}, puk_{BID}, puk_{BID} and\ M_{BID})$ as input. Then, the concerned block is accepted with access token or rejected as output. Fig.9 shows the sequence diagram for granting access to append new block into Blockchain platform.

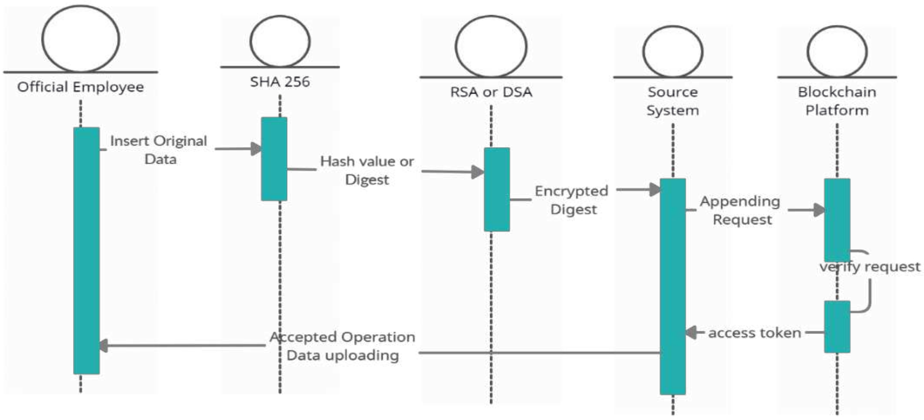


Figure 9. Sequence diagram for granting access to append new block into Blockchain platform.

Algorithm 1: Generate block signature

Input: $BID, puk_{BID}, prk_{BID}, prime\ q, M_{BID}$
Output: Signature S

```
Start Procedure
Initial $S \leftarrow null$
$if\ BID\ then$
    $Hv_{BID}$= SHA.new ($M_{BID}$). digest ()
    $k$= random. StrongRandom (). rand (1,  $puk_{BID}.q - 1$)
    $S1_{BID} = (puk_{BID})\ Sign(Hv_{BID}, k, M_{BID})$
    $S2_{BID} = (prk_{BID})\ Sign(Hv_{BID}, k, M_{BID})$
    $S_{BID} = S1_{BID} \vee S2_{BID}$
    Return $S_{BID}$
End IF
End Procedure
```

Algorithm 2: Verify request and grant access

Input: $BID, puk_{BID}, prk_{BID}$, Signature S, Source, M_{BID}
Output: Status (SS) and access token (AT)

```
Start Procedure
Initial $SS \leftarrow reject, AT \leftarrow 0$
$if\ \ puk_{BID} \wedge prk_{BID} \in S\ \ then$
    $policy_{BID}$= JSON.GetPolicy(Source.$BID$)
    $Ledger_{Log}.update(policy_{BID})$
    $AT = rand$ ()
    $issue_{time} = time.now()$
    $expire_{time} = 3600$
    SS = Approved
    Return $AT\ and\ SS$
End IF
End Procedure
```

3.3. Verification Phase

In this phase, the destination needs to verify the seal on the document. So, the destination can grant access the seal on the document and QR code. The following steps can be used to verify seal on smart document as shown in fig.10:

- Step 1: Seal on smart document and QR code generated by source are received by destination.
- Step 2: QR code is scanned to get unique ID to grant access and retrieve the unique block using this ID.
- Step 3: After a successful granting access of the unique block from Blockchain platform, the destination uses the public key associated with this block to decrypt the hash value (digest).
- Step 4: The received seal or smart official document is entered on the same hash function to produce the new hash value (new digest).
- Step 5: The outputs from the step 3 and step 4 are compared together.
- Step 6: if the comparison output is equal then the seal or smart document is accepted. Otherwise, the seal or smart document is rejected.

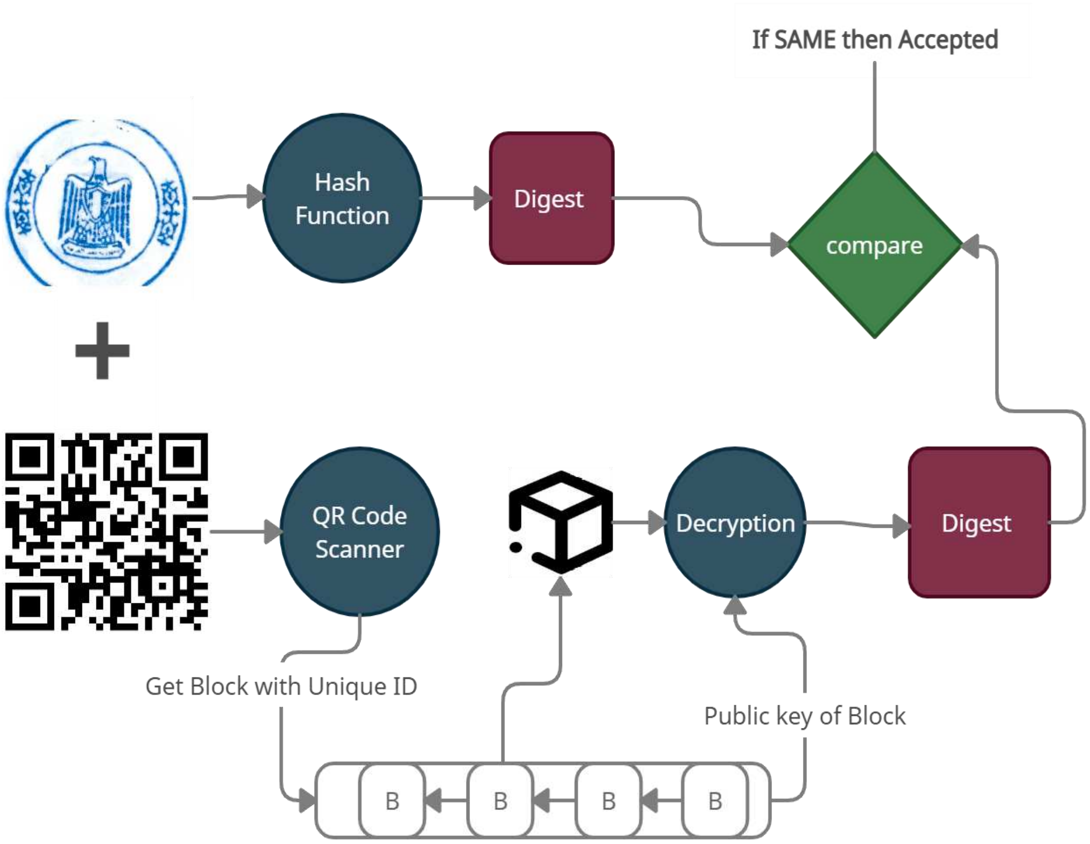


Figure 10. Steps of the verification phase.

4. Experimental Results

4.1 Dataset

We have used many images of different Egyptian governmental stamp seal imprints, which we are authorized to use by the governmental Egyptian Forensic Medicine Authority – Forgery and Counterfeiting Department, to conduct experiments, extract results, and detect fraud. This is a real sample of the Egyptian governmental Stamp Seal as represented in fig.11.

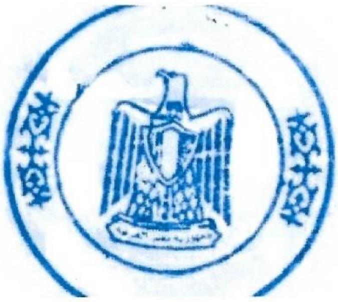


Figure 11. Sample of the Egyptian governmental stamp seal imprints after erasing all its data because of confidentiality.

4.2 Implementation Environment

At source phase. We use system with the following hardware configuration in table IV. At the Blockchain platform, we use different Blockchain platforms such as Azure Blockchain Workbench, Ethereum and Hyperledger platform. This tools permit inventors to deploy a blockchain ledger with a collection of appropriate services to evaluate different parameters on Blockchain platform such as CPU, network, and Disk usage. In this manuscript, different numbers (5, 50, 100, and 200) of nodes or peers were used. Many programs were operated at the verification phase, such as Oracle Virtual Box 6.0, Kali Linux 2018.2 vbox-i386, x, QR-Code Studio 1.0, and openssl library in Linux. The digital certificate was constructed using the 4096-bit RSA private key. After the digital certificate generation, the digital certificate and a unique ID of the smart document or stamp seal imprint file are delivered to the QR code generator.

Table IV – Source hardware configuration

Item	Specification
CPU	Intel Core ® i7 2.4 GHz
RAM	16 GB RAM
Hard disk	1 TB
Operating System	Windows 10 , CentOS

4.3 Evaluation Metrics

In this manuscript, the experimental data utilized is more than 1 million transactions from more than 400 blocks. We compare creation time of block and transaction throughput of our proposed model with Bitcoin model which is remarkably better than Bitcoin. The following metrics are used to evaluate our model:

- *QR code Readability:* The QR code readability depends on different parameters such as file size, compression rate, hash length, and execution time. Note, the input data can be of any size, while the output hash value is fixed ratio of the original data.

- *Transaction Throughput*: is the rate at which the blockchain executes valid transactions in a specified time period.

$$Transaction_{\ throughput} = \frac{Total\ committed\ Transactions}{Total\ time\ of\ seconds} \qquad (2)$$

- *Creation time of block*: is the time it carries the validators within a network to demonstrate transactions within one block and create a new block in that blockchain. The identical amount of time it carries for block generation differs and relies on the ordeal of the hash. Bitcoin takes around 10 minutes, while Ethereum only takes around 14 seconds.

- *Read Throughput*: is a calculation of how numerous read processes are conducted in a defined time period. Read processes differ from transactions in that there is no change to the state.

$$Read_{\ throughput} = \frac{Total\ Read\ Operation}{Total\ time\ of\ seconds} \qquad (3)$$

- *Query:* is the ability to run ad-hoc operations or searches against the dataset contained within the blockchain.

4.4 Results

4.4.1 Generation of QR code using different files

4.4.1.1 Testcase I (File size: 62960 bits with different compression ratio and different hash-length)

Table V – Result of the testcase I with *File size (62960 bits)*

Iteration	180	150	120	115
Compression rate	16	32	48	64
Hash length	15	31	48	64
Execution Time (seconds)	0.886	0.926	0.933	0.918
QR				

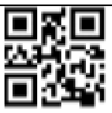
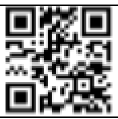
4.4.1.2 Testcase II (File size: 77630 bits with different compression ratio and different hash-length)

Table VI – Result of the testcase II with *File size (77630 bits)*

Iteration	162	125	105	93
Compression rate	16	32	48	64
Hash length	16	32	46	63
Execution Time (seconds)	1.038	1.024	1.015	1.003
QR				

4.4.1.3 Testcase III (File size: 12715 bits with different compression ratio and different hash-length)

Table VII – Result of the testcase III with *File size (12715 bits)*

Iteration	177	140	118	110
Compression rate	16	32	48	64
Hash length	15	32	46	64
Execution Time (seconds)	0.758	0.714	0.626	0.583
QR				

4.4.1.4 Testcase IV (File size: 84947 bits with different compression ratio and different hash-length)

Table VIII – Result of the testcase IV with *File size (84947 bits)*

Iteration	225	190	182	173
Compression rate	16	32	48	64
Hash length	15	32	48	64
Execution Time (seconds)	1.373	1.296	1.227	1.188
QR				

4.4.2 Transaction throughput

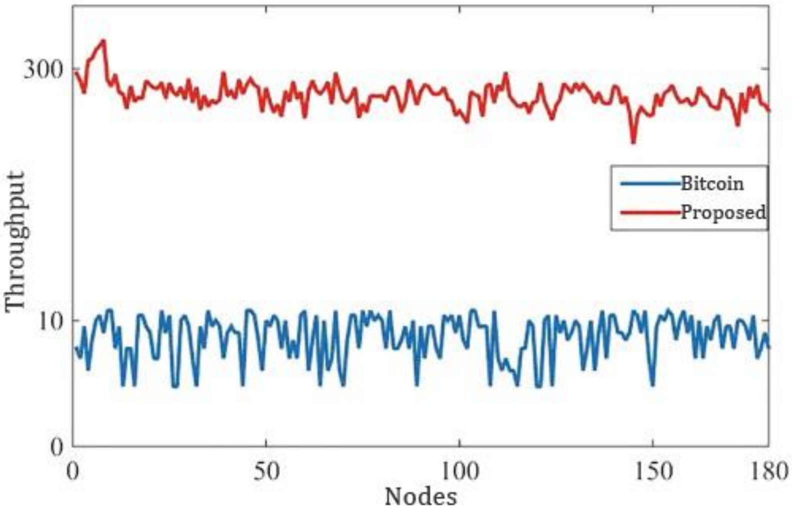


Figure 12. Transaction Throughput.

4.4.3 Creation time of blocks

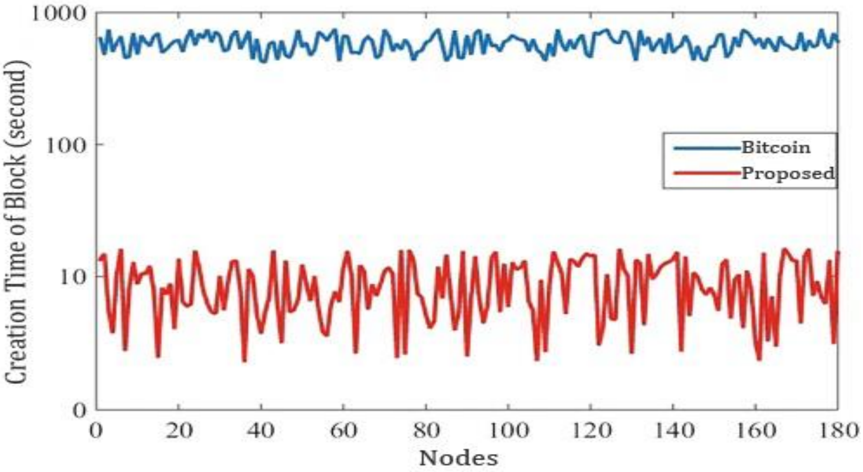


Figure 13. Creation time of Block.

4.4.4 Query time of 100 transactions

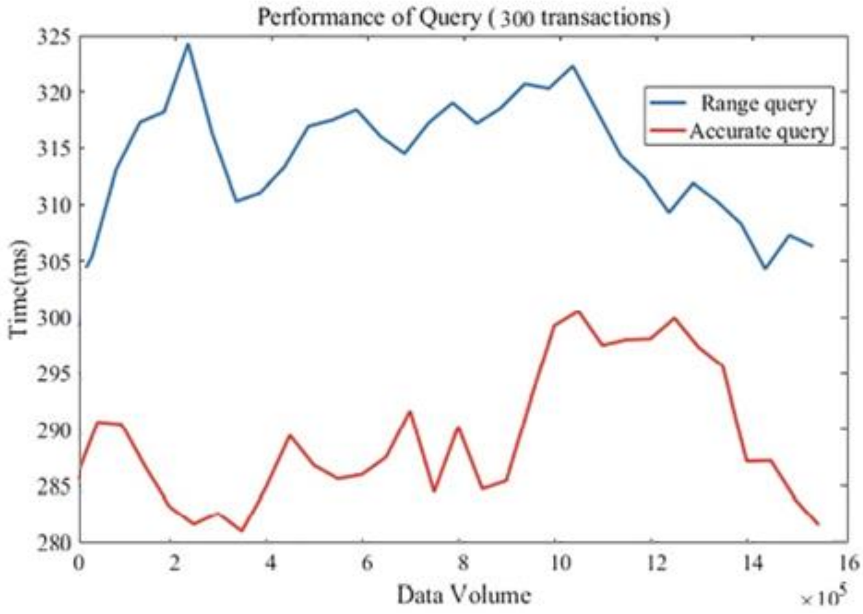


Figure 14. Query time of 300 Transactions.

4.4.5 Read Performance

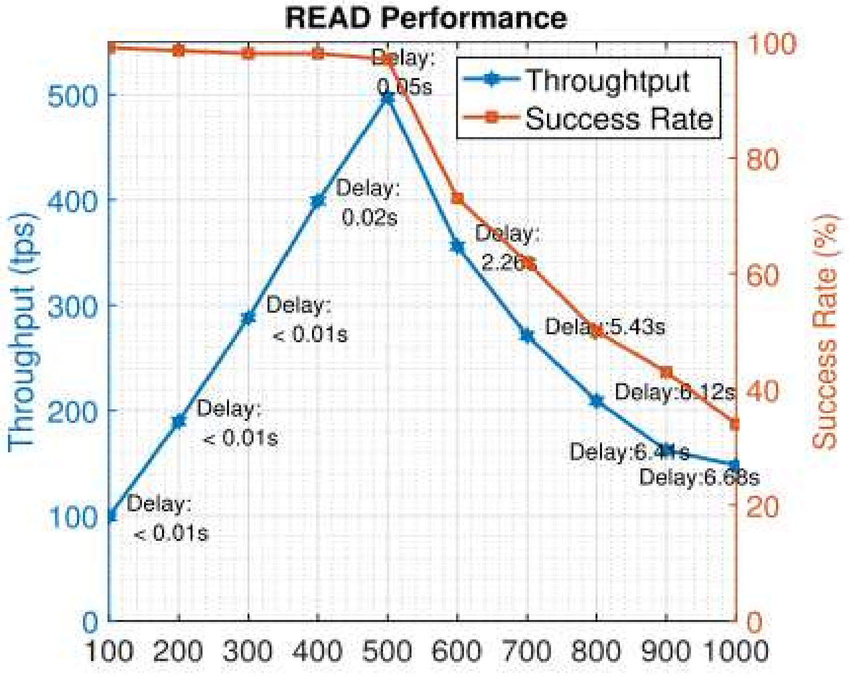


Figure 15. Read performance using different workload.

4.5 Discussion

Because our data needs a high level of security, high availability, and fast storage system, we used our proposed model to ensure the availability of data anywhere and at any time in a secure manner. An appropriate method of data compression was also used to keep transactions fast and easy to store. The quick response code was also used to link the secured electronic system (Complete digitalization) with the traditional paper system (Partial Digitalization) to obtain the advantages of the two systems. We have done many experiments and identified some testcases. Test files were uploaded including the governmental stamp seal imprints of Egypt in different sizes to evaluate accuracy. For example, we compared different testcases in section 4.4.1 with a fixed compression threshold value 64. In testcase I, we found when a file with a size of 62960 bit was used, the resulting hash size (64 digit) needed to complete this hash is 115 cycles with execution time is 0.918 seconds as shown in Table V. However, in testcase II, when we used a file with a size of 77630 bit, the resulting hash size (63 digit) needed to complete this hash is 93 cycles with execution time is 1.003 seconds as shown in Table VI. In this case, we found that the time was increased, and the hash size was reduced little bit compared with the previous testcase according to the size of the file. Also, in testcase IV, when we used a file with a size of 84947 bit, the resulting hash size (64 digit) needed to complete this hash is 173 cycles with execution time is 1.188 seconds as shown in Table VIII. The proposed model is a robust model that uses one-way encryption to generate a secure QR code and ensure data integrity. Various nodes or peers were used in this manuscript. Practically, we use transaction throughput as an evaluation metric. We found that the transaction throughput approximated three hundred per second, as shown in fig.12. Also, the creation time of a block was compared with Bitcoin, which Bitcoin gets an average 7 transactions per second, as demonstrated in fig.13. However, the query range and several query statements were used to calculate the average query time. fig.14 shows the efficiency of the system used by calculating the performance of the query using 300 transactions.

4.6 Final representation of the secured document

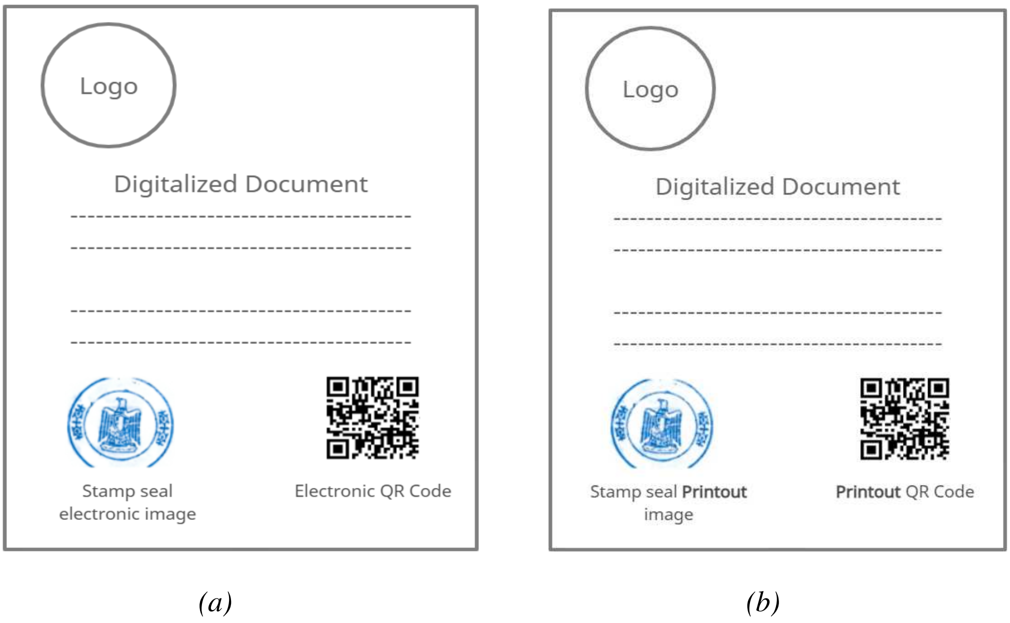


Figure 16. Final representation of secured document. (a) Secured document representation on a complete digitalization electronic system. (b) Secured document representation on a partial digitalization printout system.

5. Conclusion and Future Work

With the rapid development of technology, the number of forged documents with forged stamp seal imprints has increased tremendously, which has led to significant security and social problems. Most of the world's governments depend on securing documents on securing stamp seal imprints through inks and issuing them through a centralized environment, which contains many challenges and problems. Central repositories may have security issues such as a single point of failure challenge, data unavailability due to central system failures, or a DoS attack. Therefore, this manuscript introduced a proposal model that avoid the issues in electronic systems (completely digitalization system) and paper systems (Partial digitalization System). Our smart model used for securing stamp seal imprints or smart documents by encrypting data and storing it as a block through the decentralized Blockchain platform. After that, a QR was created to access that block quickly and securely. The proposed model was a robust model that uses one-way encryption to generate a secure QR code and ensure data integrity. After several experiments, the results proved an accuracy and security rate of stamp seal and documents that reached 98%, with a high retrieval speed compared with other related systems. In future work, we suggest to use other dataset (preferring IoT data) and evaluate accuracy. Also, we suggest to evaluate our model against different attacks such as DoS, phishing and forgery attacks such as these attacks demonstrated in these references [29,30].

DECLRATIONS

- Ethics approval and consent to participate: Not applicable.
- Consent for publication: Not applicable.
- Competing Interests: Authors have no competing interests.
- Funding: Not applicable. This research received no specific grant from any funding agency.
- Authors' Contributions: All authors read and approved the final manuscript.
- Acknowledgements: Not applicable.
- Availability of data and material: on request.

References

1. Lin SY, Zhang L, Li J, Ji L li, Sun Y. A survey of application research based on blockchain smart contract. Wirel Networks [Internet]. Springer; 2022 [cited 2022 May 7];28:635–90. Available from: https://link.springer.com/article/10.1007/s11276-021-02874-x

2. Haveri P, Rashmi UB, Narayan DG, Nagaratna K, Shivaraj K. EduBlock: Securing Educational Documents using Blockchain Technology. 2020 11th Int Conf Comput Commun Netw Technol ICCCNT 2020. Institute of Electrical and Electronics Engineers Inc.; 2020;

3. Zheng W, Zheng Z, Chen X, Dai K, Li P, Chen R. NutBaaS: A Blockchain-As-A-Service Platform. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2019;7:134422–33.

4. Wang M, Xu C, Chen X, Zhong L, Wu Z, Wu DO. BC-Mobile Device Cloud: A Blockchain-Based Decentralized Truthful Framework for Mobile Device Cloud. IEEE Trans Ind Informatics. IEEE Computer Society; 2021;17:1208–19.

5. Alhazmi HE, Eassa FE, Arabia S. BCSM: A BlockChain-based Security Manager for Big Data. IJACSA) Int J Adv Comput Sci Appl [Internet]. [cited 2022 Sep 4];13:2022. Available from: www.ijacsa.thesai.org

6. Sayeed S, Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Appl Sci 2019, Vol 9, Page 1788 [Internet]. Multidisciplinary Digital Publishing Institute; 2019 [cited 2022 Sep 4];9:1788. Available from: https://www.mdpi.com/2076-3417/9/9/1788/htm

7. Agung AAG, Handayani R. Blockchain for smart grid. J King Saud Univ - Comput Inf Sci. Elsevier; 2020;

8. Alghamdi TA, Ali I, Javaid N, Shafiq M. Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism Based on Blockchain. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020;8.

9. Singhal A, S. Pavithr R. Degree Certificate Authentication using QR Code and Smartphone. Int J Comput Appl. Foundation of Computer Science; 2015;120:38–43.
10. Yermack D. Corporate Governance and Blockchains. Rev Financ [Internet]. Oxford Academic; 2017 [cited 2021 Dec 15];21:7–31. Available from: https://academic.oup.com/rof/article/21/1/7/2888422
11. Sullivan C, Burger E. E-residency and blockchain. Comput Law Secur Rev. Elsevier Advanced Technology; 2017;33:470–81.
12. Pongnumkul S, Siripanpornchana C, Thajchayapong S. Performance analysis of private blockchain platforms in varying workloads. 2017 26th Int Conf Comput Commun Networks, ICCCN 2017. Institute of Electrical and Electronics Engineers Inc.; 2017;
13. Xu Y, Zhao S, Kong L, Zheng Y, Zhang S, Li Q. ECBC: A High Performance Educational Certificate Blockchain with Efficient Query. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) [Internet]. Springer, Cham; 2017 [cited 2021 Dec 15];10580 LNCS:288–304. Available from: https://link.springer.com/chapter/10.1007/978-3-319-67729-3_17
14. Saha G. DSign digital signature system for paperless operation. Proc 2017 IEEE Int Conf Commun Signal Process ICCSP 2017. Institute of Electrical and Electronics Engineers Inc.; 2018;2018-January:324–8.
15. Nguyen DH, Nguyen-Duc DN, Huynh-Tuong N, Pham HA. CVSS: A blockchainized certificate verifying support system. ACM Int Conf Proceeding Ser. Association for Computing Machinery; 2018;436–42.
16. Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. Proc 4th IEEE Int Conf Appl Syst Innov 2018, ICASI 2018. Institute of Electrical and Electronics Engineers Inc.; 2018;1046–51.
17. Khan SN, Shael M, Majdalawieh M. Blockchain technology as a support infrastructure in E-Government evolution at Dubai economic department. PervasiveHealth Pervasive Comput Technol Healthc. ICST; 2019;124–30.
18. Xu C, Yang H, Yu Q, Li Z. Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain. 2019 IEEE 5th Int Conf Comput Commun ICCC 2019. Institute of Electrical and Electronics Engineers Inc.; 2019;1237–42.
19. V S. SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN. J Ubiquitous Comput Commun Technol. Inventive Research Organization; 2019;01:45–54.
20. Geneiatakis D, Soupionis Y, Steri G, Kounelis I, Neisse R, Nai-Fovino I. Blockchain Performance Analysis for Supporting Cross-Border E-Government Services. IEEE Trans Eng Manag. Institute of Electrical and Electronics Engineers Inc.; 2020;67:1310–22.
21. Bharadi VA, Ghag PP, Chavan SR, Gawas SS, Kazi A. Integrating Blockchain with Local Public Service System. Springer, Singapore; 2020 [cited 2021 Dec 15];93–103. Available from: https://link.springer.com/chapter/10.1007/978-981-15-4542-9_9
22. Xie R, Wang Y, Tan M, Zhu W, Yang Z, Wu J, et al. Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System. IEEE Internet Things Mag. Institute of Electrical and Electronics Engineers (IEEE); 2020;3:44–50.
23. He H, Zheng L han, Li P, Deng L, Huang L, Chen X. An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-centric Comput Inf Sci [Internet]. Springer Science and Business Media Deutschland GmbH; 2020 [cited 2022 May 7];10:1–19. Available from: https://hcis-journal.springeropen.com/articles/10.1186/s13673-020-00255-5
24. Sun J, Yao X, Wang S, Wu Y. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020;8:59389–401.
25. Gao Y, Pan Q, Liu Y, Lin H, Chen Y, Wen Q. The Notarial Office in E-government: A Blockchain-Based Solution. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2021;9:44411–25.
26. Mohammed Ali A, Farhan AK. Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020;8:27448–58.
27. Fan C, Ghaemi S, Khazaei H, Musilek P. Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access. Institute of Electrical and Electronics Engineers Inc.;

2020;8:126927–50.
28. Guo H, Yu X. A Survey on Blockchain Technology and its security. Blockchain Res Appl. Elsevier; 2022;100067.
29. Fetooh HTM, El-Gayar MM, Aboelfetouh A. Detection Technique and Mitigation Against a Phishing Attack. Int J Adv Comput Sci Appl [Internet]. The Science and Information (SAI) Organization Limited; 2021 [cited 2022 May 7];12:177–88. Available from: www.ijacsa.thesai.org
30. Hikal NA, El-Gayar MM. Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique. Lect Notes Networks Syst [Internet]. Springer; 2020 [cited 2022 May 7];114:89–102. Available from: https://link.springer.com/chapter/10.1007/978-981-15-3075-3_6