Baghdad Science Journal

Volume 22 | Issue 6 Article 27

6-24-2025

A Feedback Management System Based on Blockchain Technology for Educational Institutions

Diman M. Mohammed
Department of Network, College of Computer and Information Technology, University of Garmian, Sulaimani, Iraq

Rana F. Ghani
Department of Computer Science, University of Technology, Baghdad, Iraq

How to Cite this Article
Mohammed, Diman M. and Ghani, Rana F. (2025) "A Feedback Management System Based on Blockchain Technology for Educational Institutions," *Baghdad Science Journal*: Vol. 22: Iss. 6, Article 27.
DOI: https://doi.org/10.21123/2411-7986.4977

BAGHDAD SCIENCE JOURNAL 2025;22(6):2073–2085

RESEARCH ARTICLE

A Feedback Management System Based on Blockchain Technology for Educational Institutions

Diman M. Mohammed [1,*], **Rana F. Ghani** [2]

[1] Department of Network, College of Computer and Information Technology, University of Garmian, Sulaimani, Iraq
[2] Department of Computer Science, University of Technology, Baghdad, Iraq

ABSTRACT

The provision of feedback is an essential element in the process of enhancing the performance of an organization. With precise feedback, errors and possibilities for improvement can be determined. The purpose of every survey is to accurately capture individuals' real feelings. Today, the majority of feedback data is stored in a database system, However, a lack of confidence in the database system results in inaccurate or partially compromised feedback. Blockchain is an innovative and promising technology that decreases security risks, eliminates fraud, and provides unprecedented levels of transparency to ensure feedback system efficiency. It is a decentralized ledger that has earned widespread attention in numerous industries. This paper investigates the use of a digital feedback management system based on blockchain technology in educational institutions that could be used to keep individual survey results safe and accurate. The proposed framework involves developing a suitable design for a feedback management system and verification of every feedback result. The system was implemented using the Java programming language. The performance of the proposed system was tested by using the number of transactions processed per second(throughput). Experimental results showed the system can verify 200 transactions in 3 seconds. In addition, the test demonstrated that the system retrieves 100–400 transactions in less than a second and 500–1000 transactions in less than 2 seconds. The throughput results were compared to the same metrics taken for several common applications. The suggested system achieved a high level of throughput when compared to several popular blockchain-based applications.

Keywords: Blockchain technology, Decentralized ledger, Educational institutions, Feedback management system, Throughput

Introduction

In the era of globalization, receiving feedback is an important component for any institution, regardless of whether it is related to commercial or academic objectives. Since the implementation of a database-based feedback system, it has gained widespread acceptance. [1] Moreover, conventional survey methodologies are susceptible to the manipulation of gathered data. [2] Blockchain's central concept is a system that guarantees records of information that are nearly impossible to alter, break, or corrupt. This will enable the elimination of any biases that may have passed into the feedback system. [1] The technology known as blockchain was introduced by Satoshi Nakamoto and has since gained significant popularity. [3] It has become a subject of significant interest among a wide array of scholars and professionals. Blockchain technology has improved over time. The current versions of blockchain are denoted as Blockchain 1.0, 2.0, and 3.0, correspondingly, and are categorized based on the types of applications they offer. [4] The technology can be traced back to Ralph C. Merkle's contributions in the 1970s when he introduced the concept

Received 21 November 2023; revised 23 March 2024; accepted 25 March 2024.
Available online 24 June 2025

* Corresponding author.
E-mail addresses: Diman.mustafa@garmian.edu.krd (D. M. Mohammed), Rana.f.ghani@uotechnology.edu.iq (R. F. Ghani).

https://doi.org/10.21123/2411-7986.4977

of the Merkle Tree.[5] The hash function of cryptography is used to encrypt and verify transactions processed by nodes. The hash value of the transaction is linked to the previous hash value. After a transaction has been placed into the blockchain, it cannot be changed or altered.[6] Blockchain technology, like in numerous other sectors, has been examined by e-government to advance the transformation of public administration and simplify the delivery of transparent and secure public services. Governments employ information and communications technology (ICT) to digitize governmental services and make them easier for residents and businesses to use. Electronic voting, management of identities, e-procurement, paying taxes, and secure transmission of information are all part of these services.[7]

The following services were examined using blockchain technology and offered by most government agencies' administrative departments: 1- Storing data in a blockchain system, and 2- Verifying the authenticity of these data.[8] However, in the actual world, the storage problem is uncertain. The majority of current blockchain apps run on simulators or small blockchain networks. The difficulty of safely storing vast amounts of data while processing verification quickly demands attention.[9]

The efficiency of the applications that are based on blockchain technology depends on a variety of parameters, which differ according to the task for which they were made. So there is no standardized way to assess the quality of a blockchain-based application. The majority of applications rely on the metric of transactions per second to illustrate the speed of transaction processing,[8] as shown in Table 1, which presents some examples of transaction rates for various apps.[10]

In this work, a mixed storage method is used, integrating blockchain with a MongoDB database, which involves securing transaction hashes on the blockchain for proof of origin. while MongoDB stores the complete raw data for efficient formatting and quick query responses.

This work aims to design and implement a secure feedback management system by utilizing blockchain technology. The proposed framework is evaluated based on the following metrics: The first aspect to consider is throughput, which refers to the measurement of accomplished transactions within a specified time. These transactions can be categorized as either requests for retrieving feedback results or verifications of the existence of a result. In addition, the system's response variability is evaluated with the increase in the number of transactions.

The rest of the paper is organized as follows: the second section presents related work and a brief overview of the background that was relied on to implement the proposed system. The third section introduces the proposed blockchain-based feedback management system. The fourth section describes the results and discussion, and the final section presents the conclusion and suggestions for future development.

Related work

This section provides an overview of prior literature reviews concerning the use of blockchain technology.

Chandratre and Garg[2] investigated the implementation of blockchain technology as a means of establishing a course feedback System for monitoring the feedback provided by students enrolled in a course. The task at hand involves the implementation of a smart contract on the Ethereum Blockchain to receive feedback from students. The survey management system will capture feedback data, which will subsequently be stored on the Blockchain to ensure its immutability and facilitate improved trackability. The authors have identified various limitations that necessitate improvement, including the validation of source data, scalability, and the need for future updates to Smart Contracts.

Ghani et al.[8] investigated protocols used in computer networks to build a decentralized system for handling government records. They provide two standard services as examples. One, using a blockchain to archive official letters, and two, using that system to verify the authenticity of such letters. The proposed structure is evaluated using two metrics: initially, throughput. Secondly, a change in portal response is proportional to the increase in transaction volume. The proposed system produced an output throughput that was comparable to that of other popular applications.

Table 1. Some blockchain-based applications used the number of transactions per second metric.[10]

Name of the Application	Number of Transactions per Second
Bitcoin (BTC)	7 TPS
Ethereum (ETH)	15–25 TPS
Litecoin (LTC)	56 TPS
Bitcoin Cash (BCH)	60 TPS

Khan et al.[11] proposed a strategy to harness the advantages of blockchain technology to establish a robust framework for electronic voting systems. The system was developed utilizing multichain, a free blockchain platform as the fundamental technology for the development of their system.

Baudier et al.[12] presented a study to examine the potential contributions of blockchain technology toward promoting global peace through the security of voting systems. The pros and cons of blockchain technology were identified through interviews with election observers and experts in the field. The findings underscore the significance of trust and human elements in the electoral procedure.

Pawlak and Poniszewska[13] aimed to present an implementation of the Auditable Blockchain Voting System (ABVS) concepts in the Hyperledger Fabric framework. The primary emphasis is on examining the organization of the e-voting blockchain network within the context of Hyperledger Fabric. The authors concluded that the aforementioned platform is well-suited for the implementation of an electronic voting system due to the presence of a distinct set of configurations that may not be present in more widely used platforms such as Bitcoin or Ethereum.

Kamal and Ghani[14] presented a blockchain-based method for government agencies to retrieve high-resolution personal data from Windows applications. This will be accomplished using smart contracts that convert transaction signing by nodes to QR codes. The suggested method was assessed based on its duration and complexity, and the algorithm was statistically analyzed; all the results were positive.

Li and Han[15] their work demonstrated the educational utility of blockchain technology. Students' records were stored using blockchain technology, and the blockchain's purpose was to ensure that the data were secure and trustworthy. In addition, data was shared using smart contracts. The evaluation of the work centered on demonstrating that the proposed system was secure and computationally efficient. For future works, the authors recommended adding capabilities to enable educational document certification for overseas institutions or employers and educational document recall.

Background

Blockchain technology

In recent years, blockchain technology has become one of the most prominent and well-known technologies. Bitcoin was the first cryptocurrency to propose and implement a blockchain.[3] It is necessary technology in the area of information and data security.[16] Blockchain is a distinct form of distributed ledger technology (DLT) that uses a network of peers to peers for saving encrypted data. It links adjacent blocks of information into chains. The entire set of information transactions on the blockchain is accessible to all participants within the network, which allows for transactions to be executed within nodes in a distributed network without requiring a trusted third party to verify the transactions.[17,18] To function properly, a distributed ledger like a blockchain network requires a consensus Procedure agreed upon by its peer nodes.[19] Consensus is a technique for validating blocks in a blockchain network by agreement amongst participating nodes, rather than a trusted third party or centralized authority.[20]

Every transaction is recorded in the blocks. Signed blocks are distributed across the network to verify the new transactions that users make. The consensus mechanism verifies the transaction and adds it to the blockchain. The miner must solve the cryptographic challenge to add the transaction to the block, and the miners receive payment for their efforts.[21] Blockchain is a series of blocks that, like a traditional public ledger, contains a full set of transaction records.[22] Every individual block within the blockchain contains a cryptographic hash value within its transaction set, as well as an additional hash value representing the preceding block in the chain.[20] The hash is generated using a Secure Hashing Algorithm (SHA). If the block is changed, the cryptographic hash changes immediately, indicating a change in the data that could be the result of a malicious action. As a result of its solid cryptographic foundations, blockchain is increasingly being used to prevent unauthorized transactions in a variety of domains.[11]

The hash of a transaction is stored in a Merkle tree, a cryptographically protected data structure.[20] It enables us to effectively demonstrate that a particular piece of data was utilized to produce a root hash regardless of requiring access to or storage of the original data. Merkle trees are built by iteratively hashing every pair of nodes till there is a single hash remaining. The Merkle root, often known as the root hash, is the summary value. Using a bottom-up method, they are built by first hashing individual transactions, then hashing the resulting pairs, and so on, until a single hash for the whole block is produced.[23]

A block refers to a set of information that is sequentially interconnected with other blocks within a digital chain. The fundamental components of a block are the block header and the transaction list. Depending on the design of the platform and the nature of the application, the header contains a variety of fields.[8]

The main attributes in the header, but not limited to, are Merkle tree root hash, timestamp: current time as seconds, nonce: a 4-byte field, which typically begins at 0 and increases with each hash computation, and parent block hash: a 256-bit hash value that indicates the block before it.[22]

There are approximately three categories of current blockchain systems: public blockchain, private blockchain, and consortium blockchain.[24]

In a public blockchain, every record is publicly accessible. In a private blockchain, only nodes from a particular organization would be permitted to participate in the consensus procedure. In contrast, only a pre-selected group of nodes would take part in the consensus process in a consortium blockchain.[25] Each block is connected to the following block of records, and a public ledger holds every committed transaction.[20] An abstract overview of blockchain structure and its blocks is shown in Fig. 1.

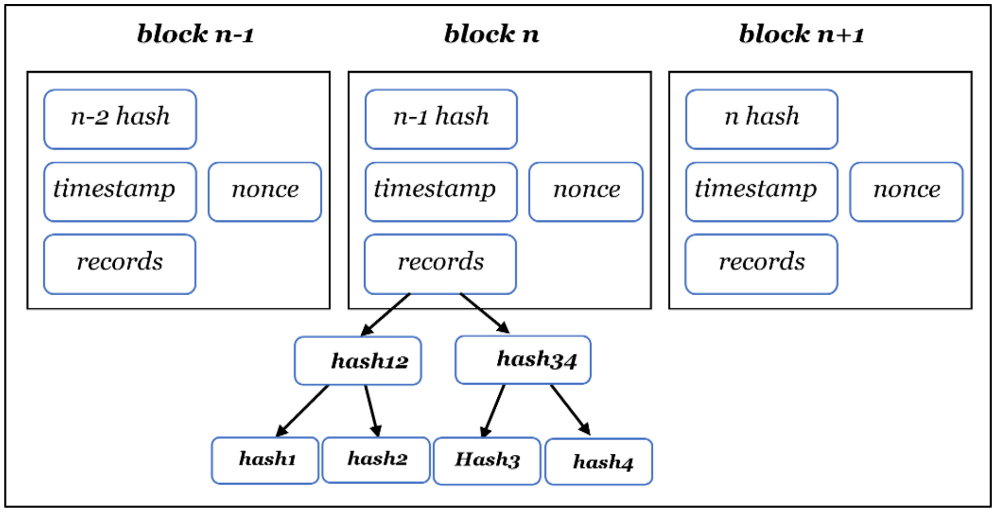

Fig. 1. A 3-block blockchainstructure example.[26]

Secure hashing algorithm (SHA)

Government organizations have recently placed a significant emphasis on data integrity. Nevertheless, confidentiality, integrity, and the availability of data may be compromised when using a computer for data processing and application due to several factors.[27] The most common methods for preserving data integrity are data backups, instituting checksums, and using hash function cryptography.[28] Hash functions, also known as message digests, generate a hash value of fixed length that is mostly unique, without utilizing a key. This hash value is produced from the original message and is similar to a fingerprint. Any minor alteration made to the message will result in a modification of the hash value. Hash functions are incapable of revealing the contents or any other attributes of the original message. However, they can be utilized to verify whether any alterations have been made to the message. Hashes offer confidentiality in this manner, but not integrity.[29] A one-way hash function, commonly referred to as a hash function, generates a fixed-length output (a hash) from an arbitrary message of any length. Given a message, it is easy to calculate the hash value using a secure hash function; given the hash value, it is challenging to reconstruct the message.[30] To assure the message's integrity, a cryptographic hash function is used to determine the message's hash value. The message's integrity may be verified at a later time by comparing the cryptographic hash function's output to the initial, stored hash value.[28] Blockchain technology ensures the security of transactions due to its robust and sophisticated cryptographic foundation, which is supported by hashing methods and timestamps.[31]

Encryption algorithms (SHA-1, SHA-2, and SHA-256) are the most widely used for blockchain technology due to their unique hash function, which generates unique outputs from various inputs.[32]

The work of the quality assurance unit

The major role of the quality assurance unit of any educational institution is primarily to initiate the feedback system and store the results for later retrieval and analysis. So, it is the manager's responsibility to safeguard the feedback system's results against tampering and alteration in the future. Hence, the feedback mechanism will work in three phases:

1. Feedback creation

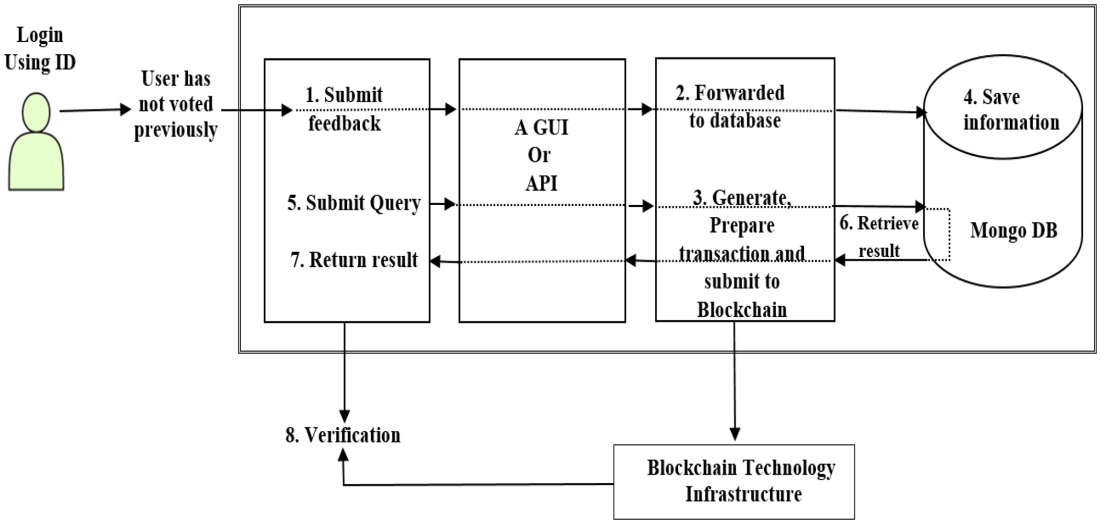

Fig. 2. The total architecture of the proposed framework in a private case.

2. Feedback recording
3. Final feedback collection and analysis.

Here, survey results can be faked or modified. The process of verifying happens to validate the retrieved feedback data before sorting the results. The cryptographic strength of the Blockchain makes the information kept there much safer. Consequently, utilizing blockchain technology to establish a local Feedback System has been proposed.

The proposed system

In the preceding section, the primary function of the quality assurance department of any government agency was described. In the following, the proposed framework for performing the same function incorporates blockchain technology.

It takes into account the following tasks:

1. Creating an appropriate design for the feedback system that can be accomplished through blockchain technology.
   – In private cases, the feedback form will be made available for registered users to make submissions using their identity numbers. The system will examine whether the provided information corresponds to a valid user.

     The first consideration will be whether the user is registered to submit feedback. The second check is performed if the user has not already voted. After passing these checks, the feedback submitted and a feedback object will be produced.
   – In public cases, the user submits feedback without registration. Subsequently, a hash value for the feedback result will be produced and stored in the blockchain. The full user information and the feedback result hash value are saved in a MongoDB database.
2. Verification of the result
   The second stage is to confirm the accuracy of the results. When it is needed to confirm the accuracy of the results, it is necessary to make a verification request to the system. If the result is present in the blockchain, it will be counted; otherwise, it will be ignored. This is accomplished by comparing the hash values of the data (result) saved in the database to the Merkle tree of the blocks in the blockchain. Figs. 2 and 3 display the total architecture of the proposed framework in both private and public cases.

The next steps provide a more in-depth explanation of the fundamental workflow.

A. Creating a list of all results' hash values.

After feedback submission, the hash value of the feedback result (transaction), as shown in Algorithm 1, is added to the Merkle tree to be verified later. while the list of transaction hashes and other detailed information like subject, and year. etc. are saved to the database.

Algorithm 1 takes an array of transactions (data). It then iterates through each transaction, calculates the SHA256 hash for each transaction, and adds the resulting hash value to (ArrayList_Hash). The final output contains all the hashed values of the transactions.

B. Appending the results to the blockchain.

The next algorithm outlines the procedural instructions for the implementation of the Merkle Tree in the

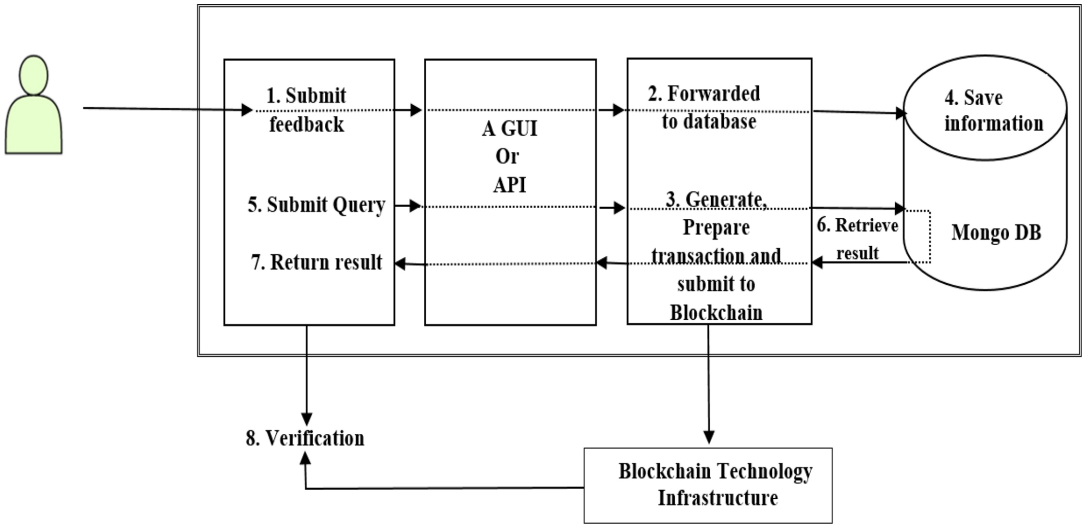

Fig. 3. The total architecture of the proposed framework in public case.

Algorithm 1: Generate a list of hash values of all the collected results (transactions).

Input:
- data (an array of transactions)
- L (length of data)

Output:
- ArrayList_Hash (an array list of hashed values)

```
Begin
  ArrayList_Hash ⇐ empty list
  for counter ⇐ 1 to L do
    Hash_value ⇐ SHA256(data[counter])
    Add(ArrayList_Hash, Hash_value)
  end for
  Return ArrayList_Hash
End
```

event of the addition of final results(transactions) to the blockchain.

Algorithm 2 starts by creating leaf nodes for each transaction and then iteratively combines pairs of nodes until a single root node is obtained, representing the Merkle Tree's root. The leaf nodes usually represent the original transactions or data. Each leaf node contains the hash value of an individual transaction.

C. Data retrieval from the database

The data retrieval process involves accessing the MongoDB database to obtain the necessary results and any additional information that may be considered necessary.

Algorithm 3 searches for a specific hash value within a MongoDB collection, provides information about whether the hash was found and displays the corresponding document if a match is found.

D. Final result Verification

At any later time, the outcome may be validated through a scan of the generated Hash Tree to ascertain its presence and a comparison between the obtained hash and the hash of the initial data saved in the DB. If the two values are similar, it is counted; else it is excluded as stated in Fig. 4 below:

Blockchain-related information and test data

The composition of a block in the proposed system involves the following components:

- Block number.
- The hash of the previous block.
- Merkle tree node.
- Time_stamps, which denote the time at which the block was hashed.

Algorithm 2: Representation for constructing a Merkle Tree.

Input:
- List of transactions (data)
- length (number of transactions)

Output:
- Merkle Tree root node

```
Begin
  if length = 0 then
    Return null
  Merkle_tree_nodes ⇐ empty array
for I ⇐ 0 to length - 1 do
  leaf_node ⇐ new Merkle_tree_node(null, null, SHA256(data[i]))
  Merkle_tree_nodes.add(leaf_node)
while length > 1 do
  new_nodes ⇐ empty array
  counter ⇐ 0
while counter < length do
  left_child ⇐ Merkle_tree_nodes[counter]
  right_child ⇐ null
  if counter + 1 < length then
    right_child ⇐ Merkle_tree_nodes[counter + 1]
if right_child = null then
    right_child ⇐ new Merkle_tree_node(null, null, SHA256(left_child.hash))
  parent_hash ⇐ SHA256(left_child.hash + right_child.hash)
  parent_node ⇐ new Merkle_tree_node(left_child, right_child, parent_hash)
  new_nodes.add(parent_node)
counter ⇐ counter + 2
  end while
  Merkle_tree_nodes ⇐ new_nodes
end while
root ⇐ Merkle_tree_nodes[0]
  Return root
End
```

Algorithm 3: Result retrieval.

Input:
- hash_value (the hash value to search for)
- Documents in MongoDB

Output:
- found (a Boolean value indicating whether the hash was found)
- Displayed Document (the document that matched the hash, if found)

```
Begin
  found ⇐ false
for counter ⇐ 1 to number of documents do
  if hash_value == hash_value in document[counter] then
    found ⇐ true
    Display Document[counter]
    Break
  Else
    found ⇐ false
  end if
end for
Return found
End
```

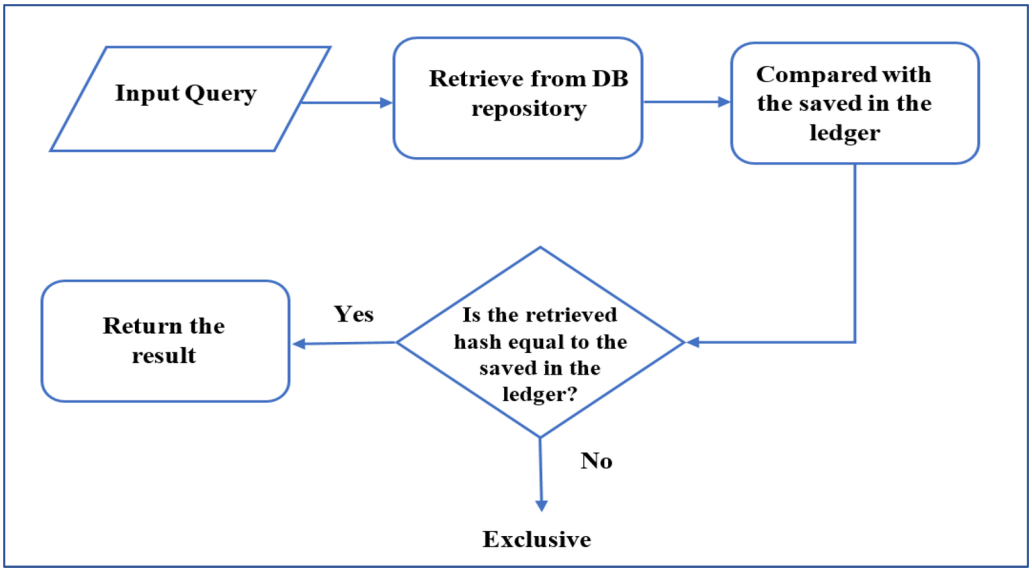

Fig. 4. The verification process.

The system has been tested using random numbers generated by a program code that helps to measure the response of the system as shown in the following algorithm:

This algorithm takes a Minimum_value (the lower bound of the range for generated numbers) and a Maximum_value(the upper bound of the range for generated numbers), then generates random numbers within a specified range. The previously obtained numerical values will be used to evaluate the performance of the implementation of the proposed system.

Result and discussion

The suggested blockchain-based feedback system services have been implemented using the Java programming language. The MongoDB database is utilized for the storage of hash values and their corresponding information. The system has been evaluated using numbers that were produced at random. Transaction verification and retrieval rates per second(throughput) were used for testing System performance.

As shown in Fig. 5, it was tested with a range of requests that started at 100 and increased up by 100 each time until it reached a maximum of 1000 requests, and the time it took to process the requests was measured in milliseconds. The Merkle tree determines whether or not a transaction can be included in a block. The verification method for transaction integrity must look for the requested transaction's hash value in each node of the blockchain's Merkle tree. The time complexity of this operation is O(log(N)), where N represents the total number of data elements. This is in contrast to a list structure, which would require O(N) time. Merkle tree scale logarithmically

Algorithm 4: The process of generating a random number for testing.

Input:
- Minimum_value
- Maximum_value
- L (number of values to generate)

Output:
- generated_numbers (an array of L random numbers)

```
Begin
generated_numbers ⟵ empty array
  for i ⟵ 0 to L do
    generated_numbers[i] ⟵ Math.random() * (Maximum_value – Minimum_value) + Minimum_value
  end for
End
```

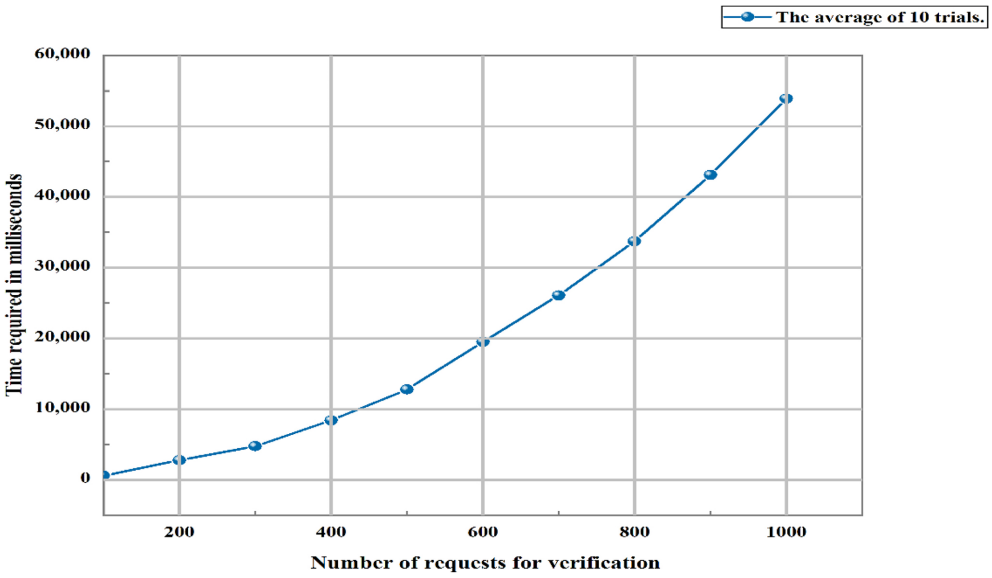

Fig. 5. The response time of 10 tests (100–1,000) verification requests.

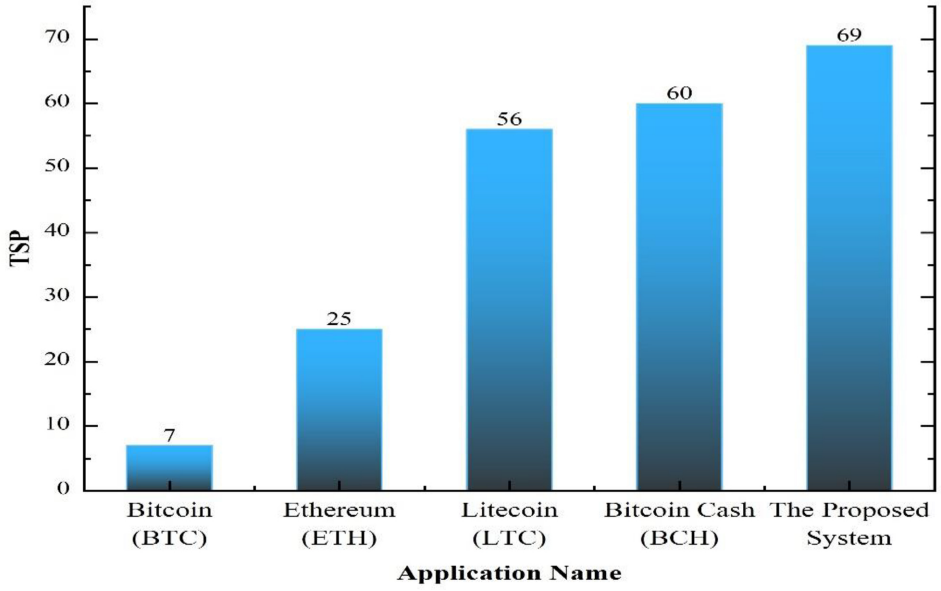

Fig. 6. Comparison between some blockchain-based applications and the proposed.

with the number of data blocks, as opposed to simply concatenating and hashing all the data at once, which would necessitate storing vast quantities of data. As a result, the time grows as the number of transactions being validated in the Merkle tree increases. The throughput of the system (which is the number of transactions processed per second) is 69 transactions per second. This is obtained by taking the average of the throughput between 100 and 1000 queries.

As compared to some common blockchain-based applications, as shown in Fig. 6, the proposed system achieves high throughput.

Fig. 7 depicts the amount of time required by the system to retrieve 100 to 1,000 requested data from the database. While MongoDB maintains a large amount of unstructured data and uses a document-based storage strategy, it facilitates faster data read and write operations. The complete personal information is kept in the database, and only the vote value, which is also stored in the blockchain, is retrieved.

The testing program was used to generate several transactions using Algorithm 4 and time functions to evaluate the responsiveness of the system. The test demonstrates that the system requires less than

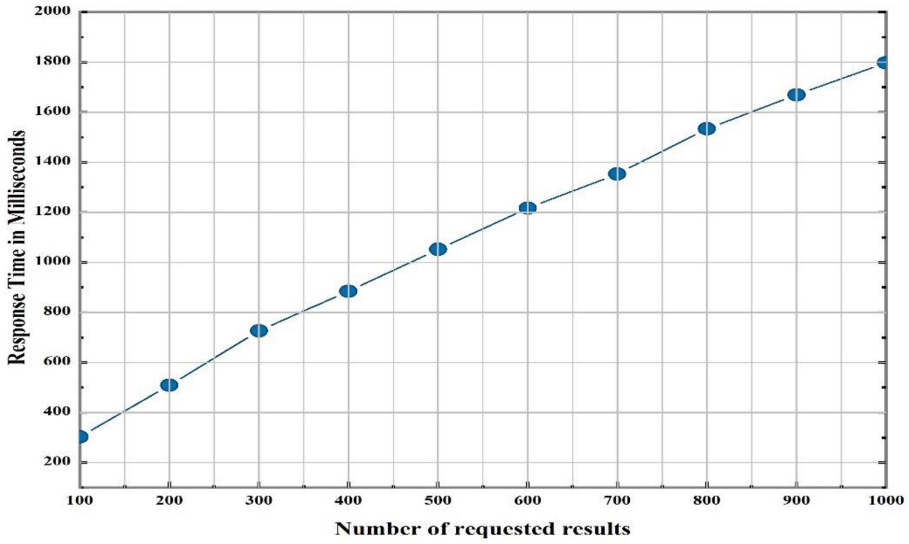

Fig. 7. Time required to retrieve feedback results based on the number of requests.

1 second to retrieve the number of transactions ranging from 100–400, and less than 2 seconds to retrieve the transactions from 500–1000. However, it can be inferred that the outcome is promising in comparison to the result in.[8]

From the tests and results described, the system is defined by the following:

- Data Integrity and Confidentiality: Information is consistently retained within the system. The information is safe from alteration with the aid of a hashing technique and timestamps.
- High Throughput: The system can process 200 transactions in about 3 seconds, which allows for a high transaction processing speed. due to the absence of the need for extensive communication or competition among nodes, faster transaction validation and throughput can be achieved.
- Quick access and data retrieval: The optimized configuration of MongoDB allows for quick access and data retrieval. MongoDB's flexibility allows it to store data without a predefined structure. make it a robust choice for saving large amounts of data.

While the system has achieved high throughput, it may also come with trade-offs; it may not provide all the benefits associated with decentralized blockchain networks, such as enhanced security through decentralization and elimination of single points of failure. As a result, the decision to deploy blockchain technology in a particular context is determined by the application or system's specific demands and goals.

Conclusion

The implementation of a secure feedback system holds significant importance in educational institutions that focus on preserving data integrity and consistency to enhance the quality of education. Blockchain technology is a very novel and useful system due to its ability to fix security vulnerabilities and prevent fraudulent activities. To ensure the safety and accuracy of the survey results, this research examines the implementation of a blockchain-based digital feedback management system within academic institutions. The integrity of the data is preserved through the use of hashing algorithms and timestamps. In addition, using MongoDB enables efficient data retrieval and access, and it is an effective way to save large volumes of data. The system's performance was evaluated through the throughput measurement. Furthermore, the response time of the system was evaluated across different request rates. The outcomes of the proposed system fell within a competitive range in comparison to other regarded blockchain-based applications. At last, as a recommendation for future work, the system can be scaled with the addition of additional nodes each one with a distinct function in a distributed way.

Authors' declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any

Figures and images that are not ours have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at the University of Technology.

Authors' contribution statement

D. M. M was in charge of experiment execution, scientific analysis, displaying results, writing the manuscript, and reviewing the article before submission. R. F. G. developed the concept for the research project and devised the methods necessary to attain a conclusive outcome.

References

1. Rahman MM, Rifat MMH, Tanin MY, Hossain N, editors. A feedback system using blockchain technology. IEEE. 3rd ICISS.2020:1114–1118. https://dx.doi.org/10.1109/ICISS49785.2020.9315989.
2. Chandratre A, Garg S. Blockchain based course feedback system. SSRN. 2019; 5. https://dx.doi.org/10.2139/ssrn.3762332.
3. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. bitcoin. 2008;23(4):1–9. https://bitcoin.org/bitcoin.pdf.
4. Xu M, Chen X, Kou G. A systematic review of blockchain. Financ Innov. 2019;5(1):1–14. https://dx.doi.org/0.1186/s40854-019-0147-z.
5. Tasca P, Tessone CJ. Taxonomy of blockchain technologies. Principles of identification and classification. Ledger. 2019;4:39. https://doi.org/10.5195/ledger.2019.140.
6. Mohammed NS, Dawood OA, Sagheer AM, Nafea AA. Secure smart contract based on blockchain to prevent the non-repudiation phenomenon. Baghdad Sci J. 2023;19. https://dx.doi.org/0.21123/bsj.2023.4618.
7. Lykidis I, Drosatos G, Rantos K. The use of blockchain technology in e-government services. Computers. 2021;10(12):168. https://doi.org/10.3390/computers10120168.
8. Ghani RF, Al-Karkhi AAS, Mahdi SM. Proposed framework for official document sharing and verification in e-government environment based on blockchain technology. Baghdad Sci J. 2022;19(6):1592-. https://dx.doi.org/10.21123/bsj.2022.7513.
9. Kumar R, Tripathi R. Large-scale data storage scheme in blockchain ledger using IPFS and NoSQL. 2021:26. https://dx.doi.org/10.4018/978-1-7998-3444-1.ch005.
10. Bach LM, Mihaljevic B, Zagar M, editors. Comparative analysis of blockchain consensus algorithms. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO); 2018:1545–1550. https://dx.doi.org/10.23919/MIPRO.2018.8400278
11. Khan KM, Arshad J, Khan MM. Secure digital voting system based on blockchain technology. IJEGR. 2018;14(1):53–62. https://dx.doi.org/10.4018/IJEGR.2018010103.
12. Baudier P, Kondrateva G, Ammi C, Seulliet E. Peace engineering: The contribution of blockchain systems to the e-voting process. Technol Forecast Soc Change. 2021;162:120397. https://dx.doi.org/10.1016/j.techfore.2020.
13. Pawlak M, Poniszewska-Marańda A, editors. Implementation of auditable blockchain voting system with hyperledger fabric. Springr ICCS 2021. 2021:642–655. https://doi.org/10.1007/978-3-030-77961-0_51.
14. Kamal ZA, Fareed R. Data retrieval based on the smart contract within the blockchain. Period Eng Nat Sci. 2021;9(4):491–507. http://dx.doi.org/10.21533/pen.v9i4.2353.
15. Li H, Han D. EduRSS: A blockchain-based educational records secure storage and sharing scheme. IEEE Access. 2019;4:179273–179289. https://dx.doi:10.1109/ACCESS.2019.2956157;7.
16. Salagrama S, Bibhu V, Rana A. Blockchain based data integrity security management. Procedia Comput Sci. 2022;215:331–9. https://dx.doi.org/10.1016/j.procs.2022.12.035.
17. Lykidis I, Drosatos G, Rantos K. The use of blockchain technology in e-government services. Computers. 2021;10(12):168. https://doi.org/10.3390/computers10120168.
18. Ballamudi KR. Blockchain as a type of distributed ledger technology. Asian J Humanity Art lit. 2016;3(2):127–36. https://dx.doi.org/10.18034/ajhal.v3i2.528.
19. Chaudhry N, Yousaf MM, editors. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. 12th Int Conf Open Source Syst Techs. 2018:54–63. https://dx.doi.org/10.1109/ICOSST.2018.8632190.
20. Ali SIM, Farouk H, Sharaf H. A blockchain-based models for student information systems. Egypt Inform J. 2022;23(2):187–96. https://dx.doi.org/10.1016/j.eij.2021.12.002.
21. Aljabr AA, Sharma A, Kumar K. Mining process in cryptocurrency using blockchain technology: Bitcoin as a case study. J Comput Theor Nanosci. 2019;16(10):4293–8. https://dx.doi.org/10.1166/jctn.2019.8515.
22. Zheng Z, Xie S, Dai H, Chen X, Wang H, editors. An overview of blockchain technology: Architecture, consensus, and future trends. IEEE 6th Int Cong Big Data. 2017:557–564. https://doi:10.1109/BigDataCongress.2017.85.
23. Bazzi A, Shaout A, Ma D. MT-SOTA: A merkle-tree-based approach for secure software updates over the air in automotive systems. Appl Sci. 2023;13(16):9397. https://dx.doi.org/10.3390/app13169397.
24. Zheng Z, Xie S, Dai H-N, Chen X, Wang H. Blockchain challenges and opportunities: A survey. Int J Web Grid Serv. 2017;14(4):352–75. https://dx.doi.org/10.1504/IJWGS.2018.095647.
25. Kaur S, Chaturvedi S, Sharma A, Kar J, He D. A research survey on applications of consensus protocols in blockchain. Secur Commun Netw. 2021;2021:1–22. https://dx.doi.org/10.1155/2021/6693731.
26. Bozic N, Pujolle G, Secci S. A tutorial on blockchain and applications to secure network control-planes. 2016 3rd Smrt Cld Net Sys (SCNS), Dubai, United Arab Emirates, 2016:1–8. https://doi:10.1109/SCNS.2016.7870552.
27. Wang X, editor Research on data integrity verification technology based on blockchain. J Phys Conf Ser. 2021. https://doi.org/10.1088/1742-6596/2035/1/012017.
28. Kleinaki A-S, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E. A blockchain-based notarization service for biomedical knowledge retrieval. Comput Struct Biotechnol J.

2018;16:288–97. https://dx.doi.org/10.1016/j.csbj.2018.08.002.
29. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography (1st ed.): CRC press; 1997.
30. Sobti R, Geetha G. Cryptographic hash functions: a review. IJCSI. 2012;9(2):461. https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review.
31. Rao TVN, Likhar PP, Kurni M, Saritha K. Blockchain: a new perspective in cyber technology. Blockchain Technology for Emerging Applications: Elsevier. 2022:33–66. https://dx.doi.org/10.1016/B978-0-323-90193-2.00004-1.
32. Kamal ZA, Fareed R. A Proposed hash algorithm to use for blockchain base transaction flow system. Period Eng Nat Sci. 2021;9(4):657–73. http://dx.doi.org/10.21533/pen.v9i4.2401.

نظام إدارة الاستبيان القائم على تقنية سلسلة الكتل في المؤسسات التعليمية.

ديمن مصطفى محمد[1]، رنا فريد غني [2]

[1]قسم الشبكات، كلية الحاسوب وتقنية المعلومات، جامعة كرميان، سليمانية ، العراق.
[2] قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة

يعد نظام الاستبيان من العناصر الأساسية لتطوير أداء المنظمة. ومن خلال الاستبيان الدقيق يتم تحديد الأخطاء معالجتها. الغرض من كل استطلاع هو الاخذ بالآراء الحقيقية للأفراد وبدقة. في الوقت الحالي، يتم تخزين اغلب بيانات الاستبيان في أنظمة قواعد البيانات، ومع ذلك، فان عدم الثقة في أنظمة قواعد البيانات تؤدي إلى نتائج غير دقيقة أو معرضة للخطر او التلاعب جزئيًا. تعد تقنية سلسلة الكتل تقنية جديدة وواعدة بشكل خاص لأنها تقلل من مخاطر الأمنية، تزيل الاحتيال، وتقدم مستويات غير مسبوقة من الشفافية التي تضمن نظام استبيان فعال. إن سلسلة الكتل دفتر لا مركزي، حظي باهتمام واسع النطاق في العديد من الصناعات. يبحث هذا البحث في استخدام نظام إدارة الاستبيان الرقمي القائم على تقنية سلسلة الكتل في المؤسسات التعليمية والذي يمكن استخدامه للحفاظ على نتائج الاستطلاع الفردي بشكل آمن ودقيق. يتضمن الإطار المقترح تطوير تصميم مناسب لنظام الاستبيان والتحقق من كل نتيجة استبيان. تم تنفيذ النظام باستخدام لغة البرمجة جافا وقيمت زمن الاستجابة لمجموعة متنوعة من الطلبات. تم اختبار أداء النظام المقترح باستخدام عدد المعاملات المنفذة خلال الثانية الواحدة (الإنتاجية). وقد أظهرت النتائج التجريبية أن النظام المقترح قام بمعالجة 400 معاملة تحقق خلال 3 ثواني. بالإضافة إلى ذلك، يوضح الاختبار أن النظام يتطلب أقل من ثانية واحدة لاسترداد عدد الطلبات التي تتراوح من 100 إلى 400 طلب. ويحتاج الى ثانيتين لاسترجاع طلبات تتراوح ما بين 500- 1000 طلب. لقد تمت مقارنة نتائج الإنتاجية بنفس المقاييس المأخوذة للعديد من التطبيقات الشائعة. حقق النظام المقترح مستوى عالي من الانتاجية بالمقارنة مع العديد من التطبيقات الشائعة المعتمدة على تقنية سلسلة الكتل.

الكلمات المفتاحية: تقنية سلسلة الكتل، دفتر الأستاذ اللامركزي، المؤسسات التعليمية، نظام إدارة الاستبيان، الإنتاجية.