Egyptian Informatics Journal 24 (2023) 100411

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Modeling of blockchain with encryption based secure education record management system

Awatef Salem Balobaid [a,*], Yasamin Hamza Alagrash [b], Ali Hussein Fadel [c], Jamal N. Hasoon [d]

[a] Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Kingdom of Saudi Arabia
[b] Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
[c] Department of Computer Science, University of Diyala, Diyala, Iraq
[d] Computer Sciences Department, College of Sciences, Mustansiriyah University, Iraq

ARTICLE INFO

Keywords:
Five-dimensional hyper chaos
Blockchain encryption
Dynamic DNA coding
Education-based Blockchain

ABSTRACT

Blockchain technology can be employed in the education sector by building a decentralized system to store and share student records. The records can be encrypted to guarantee their confidentiality and security. With a blockchain-based system, student records can be saved in blocks that are linked and secured via cryptography. The records are decentralized and not controlled by any single entity, making them less susceptible to hacking or tampering. By using blockchain technology, educational institutions can create a more secure and efficient system for storing and sharing student records. This can streamline the process of transferring records between schools, and provide a secure and transparent way for students to access their own records. In this study, we provide a novel Merkle tree-based strategy for preserving the accuracy of student records and outline how to put it into practice. The software architecture resembled blockchain technology and was developed for private network deployment. The key components of our strategy are replacing conventional audit trails with their cryptographically secure equivalent and simplifying the Blockchain framework by avoiding mining. The cryptography system's framework is presented, and the new five dimensions of chaotic map academic records are proposed. Our study utilizes deoxyribonucleic acid (DNA) sequences and operations and the chaotic system to strengthen the cryptosystem in the blockchain authentication and authorization process. The significant advantage of this method is enhancing the generation of the hash function, which is the most critical challenge in the blockchain concept. The experimental outcomes and security analysis demonstrated that the proposed method works well in terms of different aspects. The suggested hash function's hash value distribution, sensitivity to tiny message modifications, confusion and diffusion qualities, resilience against birthday attacks, key-space analysis, collision resistance, efficiency, and flexibility were all considered throughout the study.

1. Introduction

Technology in the education system is developing quickly because of the development of computer networking and information. A collaborative team could benefit from some intelligence exchange via an e-learning system in addition to teaching and learning, Blockchain is frequently employed as one of the newest technologies in distributed environments since it makes it easier to construct complex systems. Because the traditional education system requires both the student and the instructor to be present at the same time, at the exact location, and at the same interval of time that is challenging to manage every time, distributed secure systems in the education field make a significant change in society [1]. Additionally, it is also true that people find less time for the conventional way of studying in today's competitive world with its rising popularity and recently emerging technology. Although learning with tools and technology has been practiced for the past ten years, many secure learning systems are still being developed and proposed. However, these systems suffer from security and complexity limitations [2]. More specifically, in terms of reliability and scalability, user trust and privacy are one of the major issues that still need more investigation in the traditional secure learning system. Additionally, these approach struggling with storage and time complexity. We suggest a secure system that maintains user privacy to create a system that does away with these limitations of existing systems. The system's security

* Corresponding author.
E-mail addresses: asbalobaid@jazanu.edu.sa (A. Salem Balobaid), yhamza@uomustansiriyah.edu.iq (Y.H. Alagrash), jamal.hasoon@uomustansiriyah.edu.iq (J.N. Hasoon).

https://doi.org/10.1016/j.eij.2023.100411
Received 19 March 2023; Received in revised form 22 August 2023; Accepted 28 September 2023
Available online 16 October 2023

lies in an abstraction layer between the user and the system and the encryption of data transferred. Blockchain technology, which records transactions in the decentralized network in a verifiable and immutable way, has recently emerged as a suitable option for secure data storage and distributed computing. Furthermore, since records are saved on every node that makes up the Blockchain, updating a record illegally on more than 50 % of the nodes is almost hard. Transparency and security are two of Blockchain's main advantages; as a result, the E-learning process is where it fits best [4]. It is possible to use smart contracts on blockchains, which are like computer programs but are stored and executed by everyone in the network autonomously. Blockchain oracles are entities what blockchain external systems, thereby permitting smart contracts to implement depending upon the inputs and outputs from the real world. These smart contracts can read and write data from the Blockchain and other sources utilizing oracles, process information, record transaction results, startup actions in systems off-chain, and more. All transactions are tamperproof and stored on the Blockchain to build trust [5]. This paper develops a blockchain-enabled node authentication scheme in an education system, which utilizes a new approach for the hash function.

Valid information, digitally signed and strongly encrypted, can be challenging to access, even for authorized users, when decisions must be made quickly. A hacker might target the network or computer system and render it unusable.

DNA-based encryption can take advantage of the complexity of biological systems to create encryption methods that resist certain types of attacks. For example, the decoding may require specific biological conditions or enzymes that attackers cannot easily replicate.

Mixing and confusion: Anarchic maps can be used in mixing and confusion processes in encryption algorithms. These processes help increase the spread of data, ensuring that each part of the ordinary text affects multiple parts of the encrypted text, making it difficult to infer the original data.

Blockchain technology completely resolves the problems thanks to its distinctive technological advantages, such as decentralization, security, transparency, immutability, trust, efficiency, and accessibility [6]. Some blockchain-based education programs exist, although most exclusively address data integrity. Blockchain technology can be employed in the educational sector to secure educational records in a distributed environment [7].

1.1. Motivation

The motivation for this study arises from the fact that the data related to the students in the education sector is important and sensitive. The presence of a super administrator who can retrieve data on general administrative structure, learning and research may be seen as a big susceptibility. In a traditional education system based on a centralized system, there are a few challenging issues that exist in storing education records [7]. Educational records normally contain sensitive data related to the students, such as their names, address, academic records, and potentially health records. Educational records can be easily accessible to authorized personnel, such as teachers, administrators, and parents. However, providing access to the wrong people or failing to provide access to the right people can lead to issues with data security and privacy. It is essential to ensure that data remains accessible, secure, and wellorganized over time, even as technology and storage methods change. The goal of new this research is to discover other ways to securely store data. According to blockchain technology; the new method can provide a more protected and trusted archive of records which represents depending on time stamps can be a big assist for all stakeholders [3]. To overcome this problem, we, therefore, need a solution. Due to the Blockchain's speed, security, and cost-effectiveness in compiling data and records like e-learning certificates, college degrees, and others, this project, built on it, provides a solution to overcome the difficulty [4].

By examining the database's entries, blockchain technology can be utilized to verify the properties [5]. Blockchain technology enhances the security of protecting intellectual rights by preventing unauthorized use of teachers' educational designs [6]. Privacy means that every node saves the entire ledger, including every piece of data but the actual identity. Users are all identified by ID numbers to protect their privacy. Since only the trader would have access to the private key, blockchain technology can secure the trader's privacy. In the case of education, only the user's private key can access all the data regarding learning experiences that have been stored on Blockchain. Others are inaccessible; therefore, blockchain technology can effectively maintain users' privacy.

1.2. Contributions

This work develops an approach that improves student and professor data confidentially and integrity supported by Blockchain. Our contribution consists of a cryptography approach to enhance the marker tree in the Blockchain. We create a hybrid method of the DNA sequence using chaotic mapping and a hash value. Our strategy is essentially dependent upon 2 methods: DNA computing and the SHA-2 hash algorithm. The popular cryptographic hashing technique SHA-1 is used for encryption. The cryptosystem generates the 256-bit external secret key K using the SHA-256 technique. Two plain data files with a single-bit difference will have utterly different hash outputs. A brief set of experimental result analysis take place to highlight the enhanced performance of the proposed model. In short, the key contributions are given as follows.

- Develop a new Merkle tree-based strategy to securely store the student records in blockchain and outline how to put it into practice.
- Design a hybrid method comprising two approaches namely DNA computing and SHA-2 hash algorithm.
- Employ DNA sequences and operations and the chaotic system to strengthen the cryptosystem in the blockchain authentication and authorization process.
- Enhance the generation of the hash function, which is the most critical challenge in the blockchain concept.
- To the best of our knowledge, we are the first to give a specific strategy for expanding the blockchain-based education system by interfering with the DNA hash and fivedimension chaotic mapping, boosting data confidentiality and integrity.

1.3. Paper organization

The organization of the paper is as follows. Section II gives an overview of different solutions used in the proposed system; section III discusses the architecture of the proposed secure learning system. Finally, section IV illustrated the experiment and discussed the results.

2. Related work

The integration of Blockchain into e-learning and the educational system has been available in the literature.

A solution that integrates a consortium blockchain amongst academic institutions with storage servers to issue, manage, and share educational records is proposed and prototyped by Li and Han [7] in their work. The main drawback is an educational data is encrypted and stored on off-chain storage servers, but the hash of this data is permanently stored on the Ethereum blockchain. Ghazali and Saleh [8] suggest a different methodology to issue and validate academic credentials dependent upon Blockchain to decrease the prevalence of certificate counterfeiting. However, the specific blockchain technology employed in this instance is not stated. Nevertheless, it is feasible to conclude that this modern technology is gaining traction and engulfing the educational area after analyzing projects and research on blockchain technology in higher education. Its implementation alters how students and

teachers interact, making education more open and individualized. A person's plan for lifelong learning is now objectively necessary, and blockchain technology offers the means to make that plan a reality. But, blockchain technology may also lead to unequal possibilities for online and offline schooling simultaneously.

Uni-Chain, the paper by Daraghmi et al., describes, prototypes, and analyzes an Ethereumbased system for issuing and managing academic certificates that can be securely accessed and shared among students, universities, and other third parties while maintaining students' privacy field [9]. It also suggests an incentive system based on academic institutions' commitment to their efforts to keep records current and create new ones. But this system suffered from storage complexity.

Islam et al. suggest and evaluate a project to distribute test questions while guarding against leak [10] On the Blockchain, questionnaires are securely encrypted with a timestamp and stored using a smart contract that controls access times. This study has some limitations naming, What kind of blockchain technology will be used is not yet known. Additionally, the authors provide a technique for selecting a test at random. With blockchain technology and smart contracts, the interaction between students and professors is supported. Ledger is the only blockchain-based technology identified as having a use case for academic publishing [11]. Smart contracts control the procedure of sharing educational records across institutions. The book also examines performance and potential attacks on the model's security. This study uses qualitative research techniques to examine blockchain technology as it is utilized in the field of archives, providing examples of its use, opportunities, and challenges archives [12]. This study examines blockchain technology as a cutting-edge method of preventing diploma forgery using qualitative systems and a discussion of 9 renowned universities. The findings demonstrate that it is feasible to integrate Blockchain Technology into the teaching and learning methods to prevent the forgery of university transcript documents. There are also some drawbacks in this respect approach's use blockchain itself without any modification.

To manage and share multimedia material in online education, Guo et al. [13] create a public and private blockchain-based infrastructure mix targeting a new application sector. It enables students to generate lifelong academic credentials of credibility, helps protect the digital copyrights of works of multimedia provided by educational institutions, and promotes the growth of a worldwide community for the sharing of educational multimedia recourses. Additionally, there have been cases of fraud using several transactions.

The researchers focused on studying schooling using standard security measures and looked for actions that deviated from the conventional course, which will add to the complexity [14]. **Use case of Blockchain in the education system.** Blockcerts, created by the MIT Media Lab and Learning Machine, is an open-source environment for producing, exchanging, and evaluating educational certificates. The educational credentials are Open Badges-compliant and recorded on the Bitcoin blockchain. Systems, Applications & Products (SAP) company created an Ethereum-based blockchain called TrueRec. The mechanism for keeping track of professional and academic credentials [9]. Toegepast Natuurwetenschappelijk Onderzoek (TNO) company in Netherlands just launched the basis for self-sovereign identity in the blockchain project. This system is made to assist in supplying official information in digital form and only share the minimum personal data required.

Merkle tree in Blockchain. Blockchains have great potential to revolutionize the way we store, exchange, and make transactions. Blockchains enable two-party transactions without requiring a reliable third party [15]. A blockchain is made by continually concatenating the hashes of the current and preceding blocks until a lengthy chain of blocks has been formed. Transactional information, a timestamp, a nonce, and the hash of the preceding block make up a single blockchain block. Any data can be used as transaction data in this situation. The nonce is a feature blockchain used to regulate the produced hash from the block and during mining [16]. A block is represented by the concatenation and hashing of all the parameters that make up it. Existing blockchains (such as Bitcoin, Ethereum, and others) are distributed, manage their structure via tokens, and employ stack-based programming languages. By merging two successive hashes from the Merkle leaf from the bottom up and continuing the procedure on each tree level until the root was obtained, whereas the final hash was stored, Merkle trees are balanced binary hash trees. Merkle trees are balanced binary trees with data at the bottom of the tree and leaf-generated hashes as parent nodes. The first publication provides further information about the Merkle tree [17].

Blockchain in Security and Privacy. Ali et al. [21] presented a new group theory (GT)-based binary spring search (BSS) technique that comprises of hybrid deep neural network (DNN) system. The presented technique effectually identifies the intrusion in the IoT network. Primarily, the privacy-preserving technology can be executed utilizing a blockchain-based technique. The security of patient health records (PHR) is one of the important features of cryptography on the Internet because of their value and significance, preferably from the Internet of Medical Things (IoMT).One of a drawback this work suffers from overhead for using DNN.

Almaiah [22] examined a novel technique utilizing Heuristic, Signature and voting detection approaches for identifying better countermeasures for detecting security and malicious threats utilizing Blockchain technology. During this method, the cluster head node utilizes the 3 detection methods with Blockchain for detecting the malicious sensor node.

In [23], Ring Signature for permissioned Blockchain-based Private Information Retrieval method was presented for improving privacy-preserving from the smart healthcare method. The presented method primarily exploits an enhanced multi-transaction mode consortium blockchain created by distinct counts of requests to health service providers for achieving maximizing selection offers dependent upon security, availability, and transparency. However, this work needs high resource availability such high power system and storage.

Mondal et al. [24] introduce an EHR management method by combining a Blockchain multisignature stamp with a private channel structure. Multi-signature stamps tackle the question of data ownership and authority. A channel assurances that every party follow a general principle for preserving the Blockchain ledger. In this case, this work needs more development in data storage.

3. Proposed hash function, blockchain address in proof-of-work

This paper aims to develop a secure academic learning model based on Blockchain. In our approach, we enhanced the authentication as a Merkle-Tree- and authorization for user data, bitcoin; both processes are proposed based on a new D- DNA hash function that generates a chaotic map [18,19]; our solution is illustrated in Fig. 1. A user may be that negligent or accidental modifications cannot happen fast with this work. The data included in a block, in this case, academic records, cannot be updated or altered once uploaded to the Blockchain. Our method enables the cryptographically secure linking of academic records using Merkle trees, which also serve as a database for audit trails.

Since a proposed framework refers to all academic operations belonging to teachers, students, and faculty members, this work concerns students' records, including grades and test forms. More specifically, the text file and numbers a data types in the authorization process in the Blockchain [20]. After the professors submit the student grades, our framework is assembled and applies the cryptography algorithm.

3.1. Proposed encryption algorithm

An encryption algorithm dependent upon a five-dimension Chaotic map is shown in Fig. 2. Chaotic maps often include control keys and are sensitive to beginning circumstances. This section suggests a new, enhanced chaotic map and establishes the chaos of the resulting

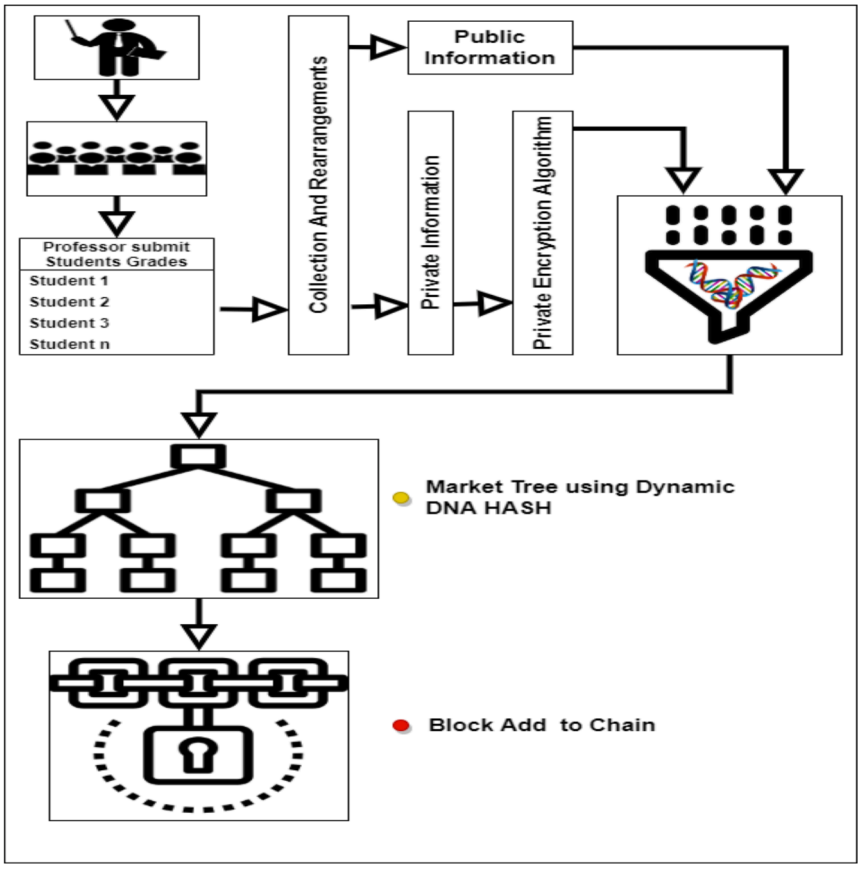

Fig. 1. Overall proposed architecture.

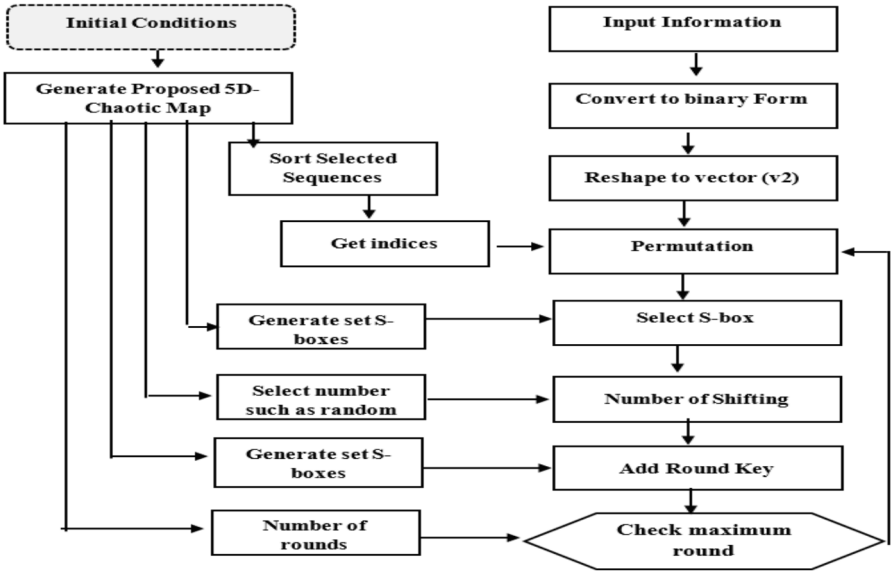

Fig. 2. Block diagram of Encryption Algorithm.

numbers. The suggested map was created using heuristics and capitalized on the advantages of the logistic map [28].

Furthermore, this map increases the dimensions and key space to develop usable user data. The extraction procedure of the proposed map was explained in the following. In the first step, the following formula is determined:

The two prerequisites listed by Shannon for a successful chaotic cryptosystem are diffusion and confusion [11,29]; both processes should be based on chaotic systems whose extreme sensitivity to beginning circumstances and parameters makes the cryptosystem incredibly secure and resistant to cryptanalysis. Although chaos is an irregular motion, it is a deterministic phenomenon, and therefore the plaintext can be recovered entirely if the secret keys are precisely known. Additionally, Encrypt, Digest and Tag (EDT) should be brief, allowing for real-time application; this necessitates that the ciphertext length is the same as that of the plaintext. The area of chaotic cryptography has made great

strides [24], but many open questions and challenges still need to be addressed before it can provide practical, efficient algorithms [25].

This paper is a phenomenon in which school policy can identify sensitive data [26]. The sensitive data should be student grades and test files with health care records that set private information and other data assumed to be public[31,32]. The student's grades represent the sensitive data that the professors scored; each student has a record, including his ID and all his grades. The incremental steps for authentication are explained as follows:

The establishment of transition for our proposed system consists of the subject teacher which collects grades for students and is called Professor Submit Students Grades for all students with their registration information. Thus, the primers are taken from the Initial Condition of each professor through which he completes work on the following steps.

The first authentication of grades per student is found in Professor Submit Students Grades based on pairing Function

The second is an encryption of each student's proposed grade algorithm. Finally, Dynamic DNA HASH is done for all students in Score Rows and the hash is extracted and called ProfHas1. All students represent the professor for this subject and with the same steps that are built for all the satin that represents ProfHas1 n. After extracting the transition for all the ProfHas Professor, we do the Collection Transition Process of Operation M. Finally, connect blockchain is done for the hash of the extruder from the Merkle tree.

3.2. Authentication and relationship Encryption

Blockchain developed the conditions required for evaluating the suitability of authentication methods for securing academic use cases. The use of blockchain technology offers a secure and reliable technique to store and share educational records, which assist in ensuring the privacy and confidentiality of sensitive student records. The utilization of Merkle hash tree authentication in blockchain assures that any transactions made on the network cannot be modified during transit, thereby maintaining the integrity of the records.

3.2.1. Pairing function

Represents an actual number as a specific convergent sequence of rational numbers. It is suitable in competitive programming as it can be simple for computing and is effectively utilized for determining the better feasible rational approximation of the underlying actual number (amongst all numbers whose denominator could not exceed a given value). Besides that, continued fractions are closely connected to the Euclidean algorithm, making them useful in many number-theoretical problems. Continued fractions are infinite sums in mathematics. Therefore, they are often handled computationally as finite sums. Here, we'll assume that all such sums end at index N. A number R represents a paring function by a simple continuous fraction (SCF).

$$R=A0+1/(A1+1/(A2+1/(A3+\ldots+1/AN))) \quad (1)$$

Where r = number of the continued fraction [27].A = number of portions in a fraction

The proposed scenario is to extract the value of the Continued fraction for each student's private data, which is to use data integrity. This method will be utilized through the authorization process; this occurs when the student's grades are taken when the encrypted text is retrieved to the explicit text, and then the Continued fraction is taken out of the explicit text, which is agreed upon at the end of the message. Therefore, the Continued fraction is extracted from the express text if it is identical and authorized if it is not considered unauthorized and has data manipulation.

3.2.2. Merkle hash tree D-DNA

As we motioned earlier, the academic record is our concern in this paper; once the professor submits student grades, the high protection approach namely hashes D- DNA function, is proposed for this purpose.

The 256-bit cryptosystem is secure against brute-force assaults. There have been numerous positive aspects of DNA computing discovered by later studies [28]. These include massive parallelism, large storage, and ultra-low power consumption. DNA cryptography is a relatively young subfield of cryptography that sprang out of the study of DNA computing; it uses DNA as an information carrier and contemporary biological technology as an implementation tool. The tremendous information density of DNA suggests it can efficiently address the one-time pad storage problem. Our method uses a chaotic map and a DNA sequence to build an impenetrable encryption system. The academic records as text and float data n are transformed using this technique's simple notion of pseudo-DNA sequence. It's an encryption method that uses a chaotic map and the XOR operation on DNA sequences.

3.2.3. DNA coding rules

The DNA sequence contains four nucleic acid bases: Adenine (A), cytosine (C), guanine (G) and thymine (T) whereas A, T and G and C are complementary, and 0 and 1 in binary are complementary [17]. Therefore 00, 01, 10, and 11 can be encoders utilizing A, C, G, and T. There are 24 encoding rules in this method, but only eight rules comply with the Watson–Crick pairing rules. The Watson-Crick base pairing rules define the particular pairing of nucleotides (adenine (A) and thymine (T), and cytosine (C) and guanine (G)) in DNA molecules. These rules were first described by James Watson and Francis Crick in their discovery of the double helix structure of DNA. The encoding methods are shown in Fig. 3. In this research, we use an encoding technique to save the genetic information of each pixel and then apply various DNA decoding procedures to alter its value. DNA encoding is more secure since it is calculated using binary operation principles. Algorithm Encoded values are created using dynamic DNA [33]. The pseudocode of dynamic DNA is shown in Algorithm 1.

Algorithm 1: Pseudocode of Dynamic DNA

```
Input: Value
  Output: Encode value binary
  Step1: initial Map DNA
  Eight types of DNA coding and decoding rules
  Step2: initial Lorenz chaotic
  Step 2: convert the value to binary
  Step 3: for each pair in binary do
  Step3-1: encoding pair
  Get x0 from 5D- Chaotic Map.
  Select-Rule =⌈⌉
  For the table get rules based on Select-Rule and pair from binary to get DNA call pair
  DNA
  Step 3–2: decoding pair DNA.
  Get x0 from 5D- Chaotic Map
  Select-Rule =⌈ ⌉
  For the table get rules based on Select-Rule and Character pair DNA in the table get
  corresponding in
  Binary
  Step3-3 end for
  Step 4: return encode value binary
```

Data with the same local value, such as having more '00′ in the plaintext, will produce more 'A' after DNA encoding according to the usual rule. When dealing with medical images, this weakness becomes more apparent. If one uses rule 1 to encode medical imagery, the most common letter in the resulting DNA arrays will be "A." Therefore, when encoding DNA, specific guidelines must be followed so that the plaintext's bit distribution is not altered. Dynamic DNA coding technology was dependent upon the position of a matrix that encoder from the data matrix P and decides for selecting the encoder rule of Table 1. That is, the DNA encoder rule of the value was computed as follows:

$$Select–Rule=[(X0*10^{!})Mod8] \quad (2)$$

X0 = the float number.

Illustrated in Fig. 4, SHA-1 needs the operation of 80 rounds that are

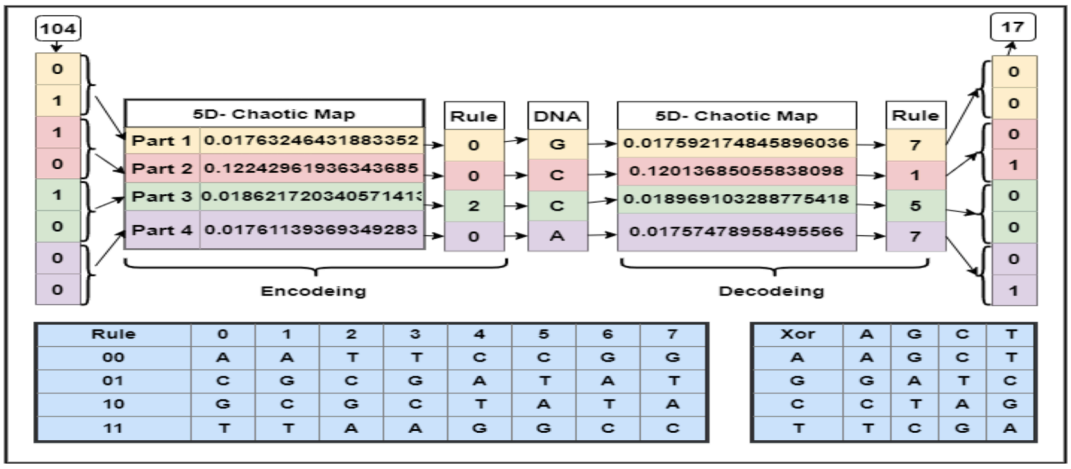

Fig. 3. DNA encoding – decoding that is used to generate eight rules for dynamic DNA hash.

Table 1
DNA rules.

Rules	1	2	3	4	5	6	7	8
0	A	A	C	C	G	G	T	T
1	C	G	A	T	A	T	C	G
2	G	C	T	A	T	A	G	C
3	T	T	G	G	C	C	A	A

grouped into four groups, 20 rounds each. Every round operates on five 32 bits hashing words (H0 to H4) with A to E as their temporary versions. Functions and constants can be basic operations of all the rounds. Those constants are round (Kt) and message word constants (Wt.).

In the proposed system, the SHA-1 is updated depending on the D_DNA of the A vector and the value for each round that needs to generate the hash. This process is done by converting two A and B to binary and encoding and decoding work. [A-DNA, B-DNA] And then [A-DNA xor B-DNA] works and the result is stored in the vector A, so the vector value is updated as shown in the algorithm in HAS-DNA

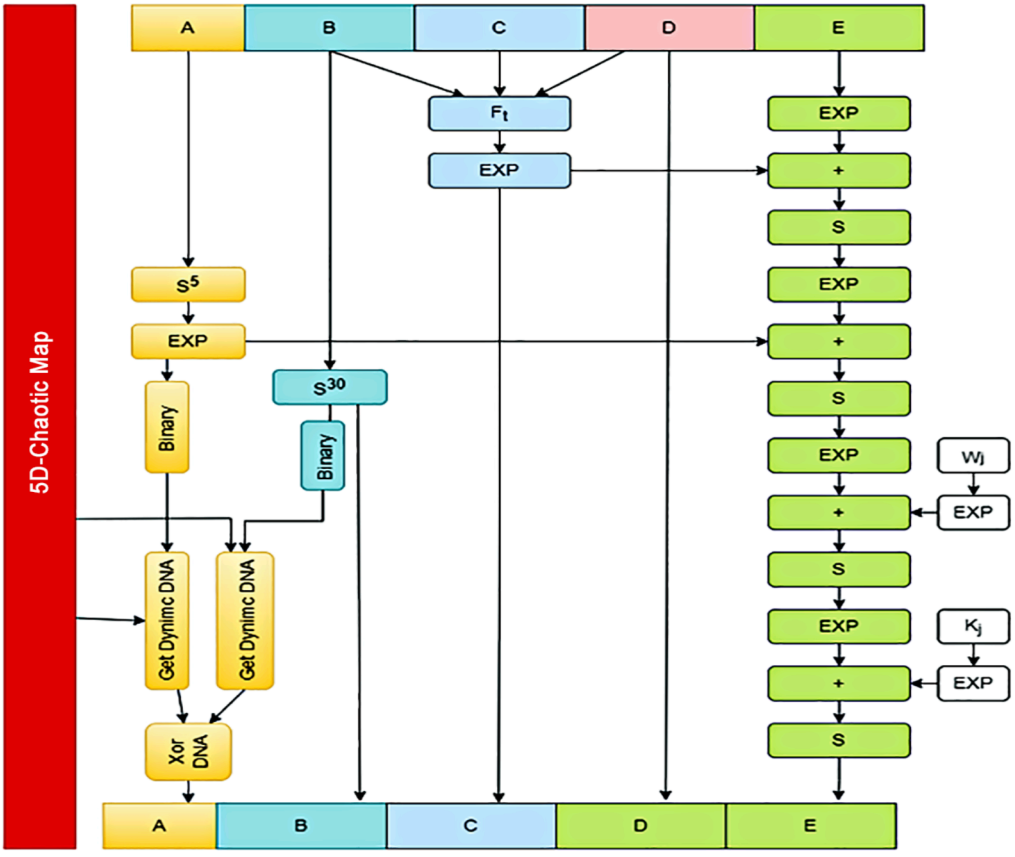

Fig. 4. Dynamic DNA hash.

Algorithm 2: HAS_DNA

Input: Data, 5D- Chaotic Map
Output: Has256 bit
Step 1: initial fixed parameters HAS
h0 = 0x67452301, h1 = 0xEFCDAB89, h2 = 0x98BADCFE, h3 = 0x10325476,
h4 = 0xC3D2E1F0 Step2: initialize:
A = H0, B = H1, C = H2, D = H3, E = H4
Step3: Perform 80 round
T = W‥ + K‥ + S#(A) + E + j(B, C,D)
E‥$% = D‥,
D‥$% = C‥
C‥$% = D‥
E‥$% =S!&(B ‥)
B‥$% = A‥,
A‥$% = T
Fort < 16;.. W‥ = W‥Andt > 17 W" =S %W "'%(⊕W"'%) ⊕ W"'* ⊕ W"'!
Step4: K‥ are variable constants given below for each i in range (0, 70):
if 0 <= i <= 9 then
f = (b and c) or ((~b) and d), k = 0x5A827999 else if 10 <= i <= 29 then
f = bˆcˆd, k = 0x6ED9EBA1 else if 30 <= i <= 49 then
f = (b and c) or (b and d) or (c and d), k = 0x8F1BBCDC else if 50 <= i <= 69 then
f = bˆcˆd, k = 0xCA62C1D6
temp = Rotate left (a, 5) + f + e + k + W[i] & 0xffffffff Step5: an update using DNA
A_Bit = convert to binary (A‥$%),
B_Bit = convert to binary (D‥$%)
DNA_a = algorithm Dynamic DNA (A_Bit, 5D- Chaotic Map)
DNA_B = algorithm Dynamic DNA (B_Bit, 5D- Chaotic Map)
A"$%= DNA_a ⊕ DNA_b Step6: Final Adds:
H& 0xffffffff H% 0xffffffff H0xffffffff
H!0xffffffff
H)0xffffffff
Step8: generation has (h0, h1, h2, h3, h4)
Step9: return HAS_DNA

above, + implies the addition with modulation reduction (viz., mod xˆ32, for any 32 bits word z=∑_(j = 0)ˆ(j = 31) a_j xˆj a_j∈{0,1}and SˆNand nS denotes n places circular left shift. Wt is calculated for word-divided padded massage.

4. Experimental results and analysis

The Ethereum platform which is an open-source platform containing smart contract (scripting) functionalities is utilized for simulation purposes. utilized the PairingFunction Solidity library to wrap the Cantor pairing function. Any Solidity contract can utilize the library by importing it using PairingFunction for uint256. Python's Flask web framework is well-liked. They are used to develop blockchain application user interfaces and APIs to communicate with the blockchain network. Making HTTP requests to communicate with other nodes on the blockchain network requires the Use Requests library. It is utilized in the decentralized network to transmit and receive data between nodes. Making HTTP requests to communicate with other nodes on the blockchain network requires the Use Requests library. It is utilized in the decentralized network to transmit and receive data between node. The experiment results are explained in this paragraph by testing the sub-models that compose the proposed system.

One part of the proposed algorithm is generating a required key in the encryption algorithm. There are several tests applied to a proposed method for evaluation. First, a method for key generation is used in the proposed method using the five-dimension chaotic system, and each dimension is processed, and the numbers seem like random numbers, as shown in Fig. 5.

The randomness test represented by NIST is used to perform the key generation method by applying the most common test and finding the p-value related to these tests, as shown in Table 2. It offers a set of statistical tests for random number generators (RNGs) for ensuring that they are producing high-quality random keys. These tests are designed to determine the arbitrariness and unpredictability of the output of an RNG, and they are a critical component of the key generation process in cryptography. In the Table 2, x, y, z, p, and k represents the keys dimension for every dimension. The obtained p value is 0.5, which is freedom degree. The attained p-value indicate that the key generated by the proposed model is acceptable.

The generated key is used to generate S-Boxes for diffusion. One sequence from the fivedimension chaotic sequence generates S-boxes used in the diffusion process. The design of cryptographically "good" S-Boxes is dependent upon essential criteria which are:

- **Balanced Criteria.** The balance criteria of the S-box are represented by the balanced distribution of the 0 and 1 values of the results. The generated S-boxes are balanced by containing numbers of 0′s equal to 1′s. This test is represented by comparing the number of zeros and the

Table 2
NIST tests for key generation.

Test Name	P-Value				
	X	Y	Z	P	K
Frequency Test	0.57825	0.59819	0.57124	0.69664	0.58226
Frequency within a Block Test	0.19819	0.43755	0.49502	0.48366	0.34889
Run Test	0.74401	0.57949	0.47088	0.60548	0.50010
Longest Run of Ones in a Block Test	0.35411	0.40138	0.33519	0.44280	0.34194
Binary Matrix Rank Test	0.46722	0.32535	0.34135	0.32481	0.33730
Discrete Fourier Transform Test	0.51863	0.65940	0.54752	0.55516	0.60388
Non-Overlapping Template Matching Test	0.54970	0.59830	0.63683	0.68445	0.61605
Overlapping Template Matching Test	0.38637	0.60548	0.43951	0.45132	0.32213
Linear Complexity Test	0.53916	0.61518	0.77480	0.72240	0.61492
Serial Test	0.60781	0.64660	0.51097	0.65850	0.58617
Approximate Entropy Test	0.54141	0.57727	0.64017	0.50789	0.48521
Cumulative Sums Forward Test	0.53528	0.63581	0.70349	0.66542	0.59038
Cumulative Sums Reverse Test	0.62763	0.54862	0.70925	0.59044	0.65525
Random Excursions Test	0.45104	0.59929	0.62095	0.57551	0.76700
Random Excursions Variant Test	0.59216	0.49392	0.52430	0.50046	40.57811

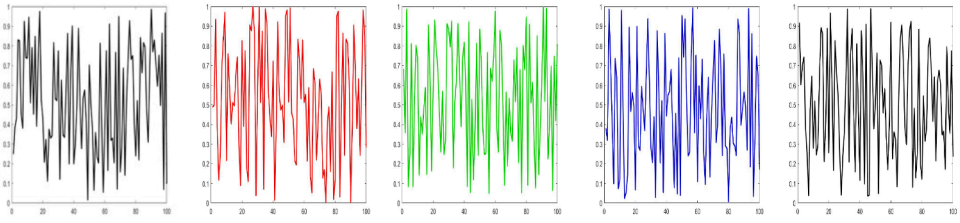

Fig. 5. The Five dimension system for key generation.

count of ones in the generated sequence. During the proposed system, the total ones equal the zeros in all generated S-box.

- **Completeness criteria.** Due to each S-dependence box on the input text, the freshly created ones met the completeness condition. The output of f(x) and f(xi) are entirely different in at least j bits if at least one combination of an eight-bit input, such as X and Xi, changes in only one bit.
- **Strict avalanche criteria (SAC).** The rigorous avalanche criteria (SAC) proposed by Webster and Tavares [38] quantifies the likelihood of bits in the output as a function of the bits in the input. The method calculates the probability that two distinct bits will be emitted when just one bit of the input data changes. The projected value would be 0.5 in an ideal world. However, the predictable value grows better closer to 0.5, indicating that S-Box satisfies the SAC requirement [38].

The avalanche property AC, which describes how a slight modification in the input bits causes a massive (avalanche) change in the output, is a crucial factor in block ciphers. This criterion, which has an ideal value of 0.5, is a characteristic that block cipher techniques might benefit from due to how it affects computational dispersion. Typically, when designing a block cipher, it is assumed the avalanche outcome but a single modification from the single bit of input results in a totally distinct output. The table illustrates the AC value of the proposed system related to the Wang et al. and Balajee and Gnanasekar methods [11] .

$$Avalanche\ Effect = (Number\ of\ Flipped\ Bits\ inOutput/(Number\ of\ All\ bits\ in\ output) \quad (3)$$

The components used to create the S-box method should have a normal distribution with a range between 0 and 1, as in Fig. 6. Equation dictates how the letters must be dispersed at the start of the procedure, and the outcome is dependent on that password.

- Bit independence criteria

The independent output bits created by Webster and Tavares provide an additional technique for assessing S-Boxes' performance [34]. This technique determines if a set of vectors produced using a plain text's reverse bit is independent of all other variable sets in an avalanche, as explained in Table 3. The correlation between avalanche variable sets is a significant factor in computing the quality of a cryptographic function's avalanche behavior and its resistance to differential cryptanalysis attacks. A correlation value can be computed to quantify the correlation between two variable sets [19]. The correlation coefficient is a widely employed statistical measure of correlation, which ranges between −1 and 1. A correlation coefficient of −1 indicates perfect negative correlation, 0 indicates no correlation, and 1 indicates perfect positive correlation. A good cryptographic function will have a low correlation between its avalanche variables. From Table 3, it is clear that the proposed model offers low correlation values. The proposed model obtains poor correlation coefficient values, which is desirable because it denotes that changing one set of input variables will result in a substantial and unpredictable change in the output, but changing another set of input variables will result in little or no change in the output. This property makes it difficult for an attacker to predict the output of the function or algorithm by modifying only a subset of the input variables.

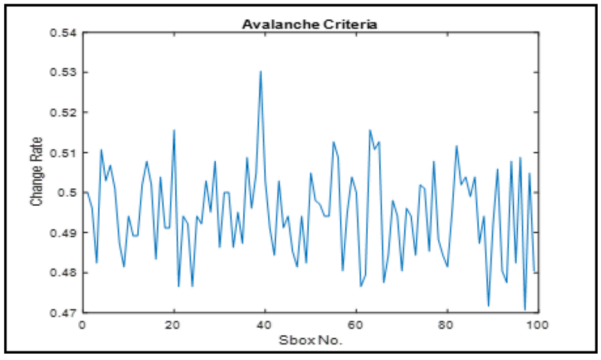

Fig. 6. The avalanche criteria of the proposed method.

Each record data are merged into a sequence of numbers used in two types of hash functions as mission before that is used in the proposed method for use in the Blockchain,

Similarity testing of two hash functions can be employed for determining the similarity or difference between the outputs of two hash functions for a given set of inputs. This type of testing is useful when comparing the performance and security of two hash functions or when attempting to determine if two hash functions are equivalent. The similarity value ranges between 0 and 1 and a value closer to zero indicates better performance.

- The Jaro-Winkler similarity is a measure of hash function similarity that compares two hash functions and calculates a score based on the number of matching characters, transpositions, and common prefixes between the two hash functions.
- The sensitivity distance, also known as the Hamming distance, is a measure of hash function similarity that compares two hash functions of equal length and calculates the number of positions at which the corresponding elements are different.
- The Levenshtein similarity, also known as edit distance, is a measure of hash function similarity that calculates the number of edits (insertions, deletions, and substitutions) required to transform one hash function into the other

Some measurements of testing two hash functions are applied in the proposed method using Jaro-Winkler similarity, sensitivity distance and normalized Levenshtein similarity [35], as explained in Table 4. From the table values, it is evident that the proposed model achieves low similarity and high sensitivity distance. A low similarity value indicates that the two hash functions produce very different outputs for the same input data, making it difficult for an attacker to guess or reverse-engineer the original data. In addition, the proposed model achieves high sensitivity distance and is desirable because it specifies that the output of the cryptographic function or algorithm is highly sensitive to variations in the input. Precisely, if the sensitivity distance of a function is high, then a small change in the input is likely to result in a significant and unpredictable change in the output, which makes it more difficult for an attacker to predict or manipulate the output.

Table 5 displays the results values of the continued fraction method used; Szudzik Pairing Functions and Cantor Pairing Functions Value [36]. Szudzik pairing functions and Cantor pairing functions are two methods for objectively mapping two positive integers to a single unique positive integer. These functions are used in various applications, such as hashing, indexing, and data compression, where a unique mapping of two positive integers is needed. The number of bits representing values has been calculated in the two ways values are converted into continued fractions, where the bit differs in the values extracted from them. As shown in the table below, the Value Cantor Pairing Functions Value method is the lowest storage of the Value Szudzik Pairing Functions.

Table 3
The correlation between avalanche variable sets.

Seq#	1	2	3	4	5	6	7	8	9	10
1	0.0000	0.0374	0.1261	0.0026	0.0034	0.0492	0.1103	−0.0381	−0.0557	0.0393
2	0.0374	0.0000	−0.0418	−0.0258	−0.0160	0.0872	−0.0734	−0.0306	−0.0355	0.0836
3	0.1261	−0.0418	0.0000	−0.0494	−0.0515	−0.0172	0.0655	0.0848	−0.1524	0.1121
4	0.0026	−0.0258	−0.0494	0.0000	0.0433	−0.0100	0.0864	0.0846	0.0194	−0.0202
5	0.0034	−0.0160	−0.0515	0.0433	0.0000	−0.0254	0.0173	0.1327	−0.0132	−0.0479
6	0.0492	0.0872	−0.0172	−0.0100	−0.0254	0.0000	−0.0409	−0.0688	−0.0160	0.0132
7	0.1103	−0.0734	0.0655	0.0864	0.0173	−0.0409	0.0000	0.0453	−0.0108	−0.0592
8	−0.0381	−0.0306	0.0848	0.0846	0.1327	−0.0688	0.0453	0.0000	−0.0023	−0.0432
9	−0.0557	−0.0355	−0.1524	0.0194	−0.0132	−0.0160	−0.0108	−0.0023	0.0000	0.0975
10	0.0393	0.0836	0.1121	−0.0202	−0.0479	0.0132	−0.0592	−0.0432	0.0975	0.0000

Table 4
Similarity test of Two hash functions.

Bin	Jarowinkler similarity (hash1, hash2)	Sensitivity distance (hash1, hash2) (Max offset = 10)	normalized_ Levenshtein similarity (hash1, hash2)
1 1.00E + 62	0.710417	26	0.175
2 1.00E + 62	0.657143	22	0.100
3 1.11E + 60	0.678736	24	0.125
4 1.00E + 63	0.603333	22	0.175
5 1.11E + 62	0.657143	26	0.100
6 1.10E + 63	0.616667	24	0.175
7 1.10E + 63	0.594444	25	0.075
8 1.01E + 63	0.612821	27	0.125
9 1.11E + 63	0.533333	23	0.100
10 1.11E + 61	0.647531	25	0.125
11 1.11E + 63	0.533333	23	0.100
12 1.00E + 63	0.586232	27	0.075

The total number of keys that can be created or utilized in an encryption process is called key space in cryptography. It indicates how many potential keys an attacker would have to sift through in order to locate the right one and unlock the data during a brute force attack. In order to prevent brute force attacks, keyspace analysis is done; the key space should be larger than 2^{128}. T is as $(10^{14})^6$ that is equal to 2^{194}, indicating that the key space is large, and the encryption scheme can withstand brute force attacks. The key space is represented by the initial parameters of the proposed system as follows: a, b, x_0, y_0, k, r where the precision of each is 10^{14}.

Therefore, this system can be trusted to generate more resistant keys to the threats. For the same reason, entering encryption and decryption processes can also be trusted. Table 6 shows the time consuming for sample of academic records in encryption and decryption transaction.

5. Discussion and evaluation

The outcome of this study provides insights into how blockchain technology along with encryption techniques was utilized in the education sector. The observed result shows how the low coefficient value prevents an attacker from predicting the value of algorithm using input variables. The blockchain technology has been used for certificate verification, to identify forgery of educational documents, and leakage of confidential information in many previous works.This method could securely store the data using DNA hashing mechanism which supports the different transactions as shown in Table 7

6. Conclusion

This architecture demonstrates how learning activities based on smart contracts, or blockchain schemas, may be verified, reliable, and traceable. This transparency feature should protect teachers that have excelled. Additionally, the school management regarding the estimation of teaching results must also be changed for embracing this novel technology—a secure education system based on Blockchain. Our framework develops a hash-function Merkle tree with a novel hash function dependent upon three proposed components: sponge construction, DNA computing and chaos. The sponge construction increases the security of the presented hash function, enabling it to extend provable security notions. DNA computing was utilized in a novel chaotic map for increasing its randomness. Novel Hash Function Based on a Chaotic Sponge and DNA sequence (resulting in improved efficiency) and security. A novel chaotic map was designed dependent upon a deterministic chaotic finite state automata configuration with four machine states and the logistic map, depicting complex, chaotic behaviours. The suggested hash function's hash value distribution, sensitivity to tiny

Table 6
Time consuming in encryption and decryption transactions.

Record no.	Enc. Time (ms)	Dec. time(ms)
1	0.00122	0.00009
2	0.00043	0.00023
3	0.00108	0.00005
4	0.00061	0.00010
5	0.00092	0.00001
6	0.00045	0.00031
Average	0.00079	0.00013

Table 5
Results of the fraction method.

#	Value	Value Szudzik Pairing Functions' with 76 bits	Cantor Pairing Functions with 73 bits
1	127,480,234,065	16,251,210,077,394,600,000,000	8,125,605,038,824,810,000,000
2	127,480,235,065	16,251,210,332,355,100,000,000	8,125,605,166,305,040,000,000
3	127,480,236,065	16,251,210,587,315,600,000,000	8,125,605,293,785,280,000,000
4	127,480,237,065	16,251,210,842,276,000,000,000	8,125,605,421,265,520,000,000
5	127,480,238,065	16,251,211,097,236,500,000,000	8,125,605,548,745,750,000,000
6	127,480,239,065	16,251,211,352,197,000,000,000	8,125,605,676,225,990,000,000

Table 7
Evaluated the proposed solution.

#	Papers	Solution	Utilization Method with blockchain
1	H. Li and D. Han [29]	To maintain data storage security, the offchain records are periodically anchored with the blockchain's hash data. Message digital signature and record encryption are handled by cryptography techniques.	Use standardized encryption and message digital signature
2	Meng Han etal, [30]	Issue academic certificate through blockchain	No development in block chain method
3	Proposed Solution	Block chain in education system using development method based on encryption with DNA- Hashing function	Modified DNA-Hash in encryption

message modifications, confusion and diffusion qualities, resilience against birthday attacks, keyspace analysis, collision resistance, efficiency, and flexibility were all considered throughout the study. The results reveal that the presented function has virtually effective statistical features compared to prior chaotic hash methods. In future, the authors plan to test the proposed techniques utilizing the smart contracts and the Ethereum network dependent upon activating the verification, authentication, and transparency of marks. In addition, there is a need for a professional platform to deploy, schedule, and manage smart contracts.

7. Institutional Review Board Statement

Not applicable.

8. Informed Consent Statement

Not applicable.

9. Ethics approval

This article does not contain any studies with human participants performed by any of the authors.

Funding

The authors acknowledge the Deanship of Scientific Research, Jazan University, Jazan, Kingdom of Saudi Arabia for funding the project. The reference number is W43-078.

CRediT authorship contribution statement

Awatef Salem Balobaid: Investigation, Writing – original draft. **Yasamin Hamza Alagrash:** Investigation, Methodology, Writing – original draft. **Ali Hussein Fadel:** Formal analysis, Validation, Writing – review & editing. **Jamal N. Hasoon:** Investigation, Software, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Gorkhali A, Li L, Shrestha A. Blockchain: a literature review. J Manag Anal 2020;7(3):321–43. https://doi.org/10.1080/23270012.2020.1801529.
[2] Svejda M, Goldberg J, Belden M, Potempa K, Calarco M. Building the Clinical Bridge to Advance Education, Research, and Practice Excellence. Nurs Res Pract 2012;2012:1–10. https://doi.org/10.1155/2012/826061.
[3] Balcerzak AP, Nica E, Rogalska E, Poliak M, Klieštik T, Sabie OM. Blockchain Technology and Smart Contracts in Decentralized Governance Systems. Adm Sci 2022;12(3). https://doi.org/10.3390/admsci12030096.
[4] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017, 10.1109/BigDataCongress.2017.85.
[5] M. Florian, S. Henningsen, S. Beaucamp, B. Scheuermann. Erasing Data from Blockchain Nodes. In: Proc. - 4th IEEE Eur. Symp. Secur. Priv. Work. EUROS PW 2019, pp. 367–376, 2019, 10.1109/EuroSPW.2019.00047.
[6] Raimundo R, Rosário A. Blockchain system in the higher education. Eur J Investig Heal Psychol Educ 2021;11(1):276–93. https://doi.org/10.3390/ejihpe11010021.
[7] Tian HJ, Lei P, Wang Y. Image encryption algorithm based on chaos and dynamic DNA coding. Jilin Daxue Xuebao (Gongxueban)/J Jilin Univ (Eng Technol Ed) 2014;44(3):801–6. https://doi.org/10.13229/j.cnki.jdxbgxb201403035.
[8] Ghazal O, Saleh OS. A graduation certificate verification model via utilization of the blockchain technology. J Telecommun Electron Comput Eng 2018;10(3–2):29–34.
[9] Daraghmi EY, Daraghmi YA, Yuan SM. UniChain: A design of blockchain-based system for electronic academic records access and permissions management. Appl Sci 2019;9(22). https://doi.org/10.3390/APP9224966.
[10] Islam A, Kader MF, Shin SY. BSSSQS: A blockchain-based smart and secured scheme for question sharing in the smart education system. J Inf Commun Converg Eng 2019;17(3):174–84. https://doi.org/10.6109/jicce.2019.17.3.174.
[11] Li H, Han D. EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. IEEE Access 2019;7:179273–89. https://doi.org/10.1109/ACCESS.2019.2956157.
[12] Noor MU. "Implementasi Blockchain di Dunia Kearsipan: Peluang, Tantangan, Solusi atau Masalah Baru?", Khizanah al-Hikmah. J Ilmu Perpustakaan Informasi dan Kearsipan 2020;8(1):81. https://doi.org/10.24252/kah.v8i1a9.
[13] Guo J, Li C, Zhang G, Sun Y, Bie R. Blockchain-enabled digital rights management for multimedia resources of online education. Multimed Tools Appl 2020;79(15–16):9735–55. https://doi.org/10.1007/s11042-01908059-1.
[14] Hewa T, Ylianttila M, Liyanage M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. J Netw Comput Appl 2021;177. https://doi.org/10.1016/j.jnca.2020.102857.
[15] Mitra D, Tauz L, Dolecek L. Polar Coded Merkle Tree: Improved Detection of Data Availability Attacks in Blockchain Systems. IEEE Int Symp Inf Theory - Proc 2022;2022-June:2583–8. https://doi.org/10.1109/ISIT50566.2022.9834538.
[16] Kan J, Kim KS. MTFS: Merkle-Tree-Based File System. ICBC 2019 - IEEE Int Conf Blockchain Cryptocurrency 2019:43–7. https://doi.org/10.1109/BLOC.2019.8751389.
[17] Zhu H, Guo Y, Zhang L. An improved convolution Merkle tree-based blockchain electronic medical record secure storage scheme. J Inf Secur Appl 2021;61(August). https://doi.org/10.1016/j.jisa.2021.102952.
[18] Guesmi R, Farah MAB. A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimed Tools Appl 2021;80(2):1925–44. https://doi.org/10.1007/s11042-020-09672-1.
[19] H. Chaotic, M. Di, D. N. A. Confusion, D. H. Elkamchouchi, and H. G. Mohamed. A Bijective Image Encryption System Based on.
[20] 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 Bioinformat) 2017;10580 LNCS:288–304. https://doi.org/10.1007/978-3-319-67729-3_17.
[21] Alawida M, Samsudin A, Sen Teh J, Alshoura WH. Digital cosine chaotic map for cryptographic applications. IEEE Access 2019;7:150609–22. https://doi.org/10.1109/ACCESS.2019.2947561.
[22] Farah MAB, Farah A, Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn 2020;99(4):3041–64. https://doi.org/10.1007/s11071-019-05413-8.
[23] Alawida M, Samsudin A, Sen Teh J, Alkhawaldeh RS. A new hybrid digital chaotic system with applications in image encryption. Signal Process 2019;160(February):45–58. https://doi.org/10.1016/j.sigpro.2019.02.016.
[24] T. Farah, S. Belghith. A new chaotic encryption algorithm for WSN and implementation with sensors ASXM1000. In: 2017 18th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2017 - Proc., vol. 2018-Janua, no. December, pp. 684–689, 2018, 10.1109/STA.2017.8314968.
[25] Li L, Abd El-Latif AA, Jafari S, Rajagopal K, Nazarimehr F, Abd-El-atty B. Multimedia Cryptosystem for IoT Applications Based on a Novel Chaotic System Around a Predefined Manifold. Sensors 2022;22(1):1–17. https://doi.org/10.3390/s22010334.
[26] Domingo-Ferrer J, Farràs O, Ribes-González J, Sánchez D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Comput Commun 2019;140–141(March):2019. https://doi.org/10.1016/j.comcom.2019.04.011.
[27] M. P. Szudzik. The Rosenberg-Strong Pairing Function. pp. 1–27, 2017, [Online]. Available: http://arxiv.org/abs/1706.04129.

[28] Mani SR. DNA Cryptography Based Secure Data Transmission. Ann Rom Soc Cell Biol 2021;25(6):655–67.
[29] S. Ramanujam, M. Karuppiah, and A. Professor, "Designing an algorithm with high Avalanche Effect," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, p. 106, 2011, [Online]. Available: http://paper.ijcsns.org/07_book/201101/20110116.pdf.
[30] M. Han, D. Wu, Z. Li, Y. Xie, J. S. He, and A. Baba, "A novel blockchain-based education records verification solution," SIGITE 2018 - Proc. 19th Annu. SIG Conf. Inf. Technol. Educ., no. September, pp. 178–183, 2018, 10.1145/3241815.3241870.
[31] Badr AM, Zhang Y, Ahmad Umar HG. Dual authentication-based encryption with a delegation system to protect medical data in cloud computing. Electronics 2019;8(2):171.
[32] Abdoun N, El Assad S, Manh Hoang T, Deforges O, Assaf R, Khalil M. Authenticated Encryption Based on Chaotic Neural Networks and Duplex Construction. Symmetry 2021;13(12):2432.
[33] Zhu S, Zhu C. Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. Entropy 2020;22(7):772.
[34] Slavin O, Farsobina V, Myshev A. Analyzing the content of business documents recognized with a large number of errors using modified Levenshtein distance. In: Cyber-Physical Systems: Intelligent Models and Algorithms. Cham: Springer International Publishing; 2022. p. 267–79.
[35] Fazio P, Mehic M, Voznak M. A deep stochastical and predictive analysis of users mobility based on Auto-Regressive processes and pairing functions. Journal of Network and Computer Applications 2020;168:102778.
[36] Dharshini S, Subashini MM. Cantor Pairing lightweight key generation for wireless body area networks. Smart Health 2022;25:100298.