Library Progress International
Vol.44, No.5, Jul-Dec 2024: P.588-601

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Enhancing E-Voting Security with Block chain and Decentralized Random Number Generation

Mays Moneer Abd Ali[1] ,prof.dr .Bashar M.Nema[2]

[1]1Department of Computer Science, Information Institute, Higher University, Iraq
[2]MustansiriyahUniversity/Department of Computer Science, Iraq

How to cite this article: Mays Moneer Abd Ali ,prof.dr .Bashar M.Nema (2024). Enhancing E-Voting Security with Block chain and Decentralized Random Number Generation. *Library Progress International,* 44(5), 588-601

Abstract:
This work addresses the challenges of security, transparency, and efficiency in modern elections by presenting a novel electronic voting system that makes use of blockchain technology, zero-knowledge proofs (ZKP), and sophisticated cryptographic methods. RSA for encryption, ZKP for voter authentication, and chaotic systems for random key generation are all part of the proposed permissioned blockchain architecture. The paper highlights the system's potential to reduce the expenses and security issues related to conventional voting methods while outlining its design, methodology, and implementation specifics. The National Institute of Standards and Technology (NIST) randomization requirements were utilized to thoroughly verify the hybrid chaotic system and modified SHA-3 algorithm that were employed in the design. The ZKP system achieved an astounding 99.8% accuracy for user verification, demonstrating remarkable levels of randomization and security. In the digital age, this all-encompassing approach to e-voting presents a viable way to have safe, open, and impenetrable elections. The system seeks to improve the voting process's dependability and integrity while encouraging increased accessibility and efficiency by integrating state-of-the-art technologies.

Keywords: Blockchain, Zero knowledge protocol (ZKP), Electronic E-Voting, Secure Hash Algorithm (SHA-3), RAS, Fisher Yates Algorithm

Introduction

A blockchain prototype with a permissioned Zero Knowledge protocol is used in this study to demonstrate an electronic voting system [1]. By lowering expenses related to staffing, polling station setup, and security threats, the method seeks to make elections more dependable, transparent, trustworthy, and cost-effective [2]. Through secure write-in voting techniques that permit uncontrolled machine updates and provide hacker protection, blockchain technology improves the accuracy and transparency of electronic voting [3]. It is dependable, eco-friendly, and lowers security and personnel.

Any democracy must include voting, and although the current system is based on a sound foundation, it is paralyzed [4]. Zero-knowledge proof protocols (ZKPs) are cryptographic protocols that enable one party to verify the truth of another without providing any extra information [5]. They are critical for building trust and privacy in digital interactions such as blockchain technology, cyber security, and data privacy [6].

The "Chaotic System with Zero Knowledge Protocol" combines the robust security of chaotic systems with the privacy and security of Austrian flag protocols [7]. Traditional voting systems, such as those used in the US, Brazil, India, Estonia, and Norway, aim to improve election efficiency, increase accuracy, and expedite the vote-counting process [8],[9].

This paper contributes to the development of systems based on Blockchain technologies by examining previous studies, system methodology, application, results, and conclusions [9].

1. Related Work

This section examines several blockchain e-voting technologies, their security, and weaknesses. Casado-Vara and Corchado suggest a blockchain system to alleviate traditional voting limits, however it has drawbacks such as high bandwidth requirements and static internet connections. Kotsiuba et al. offer a decentralized network for e-health services based on the Exonum blockchain, although both schemes have security weaknesses such as insider and impersonation attacks [9].

Kartik Hegadekatti [10] suggested "Democracy 3.0" in 2016, storing votes on a public blockchain for transparency, anonymity, and verifiability. Anyshchenko et al. presented a cryptocurrency token-based application in 2019, however it delivered poor service. Dhulavvagol et al., as well as Chauhan et al. in 2019, emphasized the need of protecting voter privacy in blockchain-based systems. Bazzi et al. advocated for hybrid systems that combine blockchain and traditional vote counting and authentication mechanisms. Hussain et al. proposed hybrid solutions to improve voting integrity and transparency [11].

hashing system, smart contracts, and Markle trees for a digital e-voting system in 2020. Ganesan et al. (2021) proposed a voting system using biometrics and RFID, while Gupta and associates (2021) used Paillier encryption for voter confidentiality [11],[12]. Blockchain technology has been used to develop various applications that utilize distributed economies. One such model is an Android application that includes extra security features including fingerprint authentication and a unique identifying key. Other initiatives include a blockchain-based biometric voting system, a private permission blockchain network, the "MATDAAN" idea, an ECC-based anonymous signcryption system, and a public blockchain-based, lightweight elliptic curve cryptography (ECC) e-voting system for Iraq. However, these systems confront several obstacles, including assaults, energy consumption, and multiple voting concerns. Neloy et al. proposed a secure and transparent electronic voting system for the United States in 2023, based on Web 3.0, reusable smart contracts, state-based blockchain technology, and AI-based multilayer authentication and verification procedures. These improvements underscore the importance of dependable, effective, and lightweight electronic voting systems that enable users to cast their ballots securely [12]. Cryptographic technologies including hash functions, encryption, digital signatures, and authentication protocols for data and devices, as well as E-voting, can help address this issue. Have been developed. These processes frequently involve. They used a pseudo-random number generator (PRNG) in the construction of important duties, such as key generation [13] .As shown here in Table 1In recent years, there has been extensive research and effort on voting systems and how to defend them with Blockchain.However, there are still difficulties to resolve, such as scalability and voter privacy. Additional research anddevelopment are necessary to create a robust and dependable blockchain-based voting system appropriate for large-scale elections. By proposing a hybrid system that combines techniques (RSA, SHA-3, chaotic system, and zero-knowledge protocol) with Blockchain technology and incorporates these techniques into the approved voting system, the chaotic system was modified to generate keys, and the hashing function in Blockchain was developed in the process. Electronic voting is used to avoid tampering with voters' votes, promote randomness and transparency by not keeping the voter's number, and to provide high security in the electronic voting process.

Table 1: Developments in Blockchain-Based E-Voting from 2016 to 2023

Year	Researchers	Title/Interest	Method Used	Advantages	Disadvantages	Suggestions/Findings
2016	Kartik Hegadekatti	Democracy 3.0	Public blockchain, Proof-of-Stake	Transparent, anonymous, verifiable, low-cost transactions, high throughput	Scalability issues, potential privacy concerns	Proposed a proof-of-stake consensus algorithm suitable for large-scale elections
2019	Anyshchenko et al.	Cryptocurrency token-based application using Tendermint and Exonum	Tendermint, Exonum	Scalability, security	Subpar service compared to PBFT	Suggested using Tendermint and Exonum for scalable and secure cryptocurrency applications

2020	Dhulavvagol et al.	Fingerprint-oriented hashing system for decentralized voting	Smart contracts, blockchain	Transparency, security, speed	Not specified	Proposed a fingerprint-oriented hashing system for enhanced security and transparency
2021	Olaniyi et al.	Multi-factor authentication in electronic voting	Feistel block cipher, smart cards	Security, tamper resistance	Not specified	Utilized multi-factor authentication and modified Feistel block cipher for secure voting
2021	Sadia et al.	Biometric electronic voting system using PBFT	Private permission blockchain, PBFT	Privacy, control, efficiency, customization, defense against DoS attacks	Biased key management	Employed PBFT algorithm within a private permission blockchain to enhance voting system security
2021	Jain et al.	MATDAAN concept using Ethereum for secure voting	Ethereum blockchain	Decentralization, upgradability, token standardization	Vulnerability to 51% attack	Proposed Ethereum blockchain for decentralized and upgradeable voting solutions
2021	Waheed et al.	ECC-based anonymous signcryption system	ECC-based signcryption	Dual functionality, flexibility	Security constraints	Focused on ECC-based signcryption for secure and anonymous electronic voting
2022	Jumaa and Shakir	Lightweight ECC e-voting system for Iraq	Public blockchain, ECC	Auditability, transparency, lightweight and efficient	Vulnerable to 51% attack, excessive energy use	Implemented QR codes, SHA-256 hashing, and PoW consensus for improved voting system
2023	Neloy et al.	Safe and transparent electronic voting system for the US	Web 3.0, smart contracts	Security, transparency, auditability, accessibility, reduced errors	Voter information management issues	Utilized Web 3.0, reusable smart contracts, AI-based authentication, and advanced methods
2019	Chauhan et al.	Issues with voter anonymity in blockchain-based systems	Blockchain-based systems	Openness, immutability	Risk of compromising voter anonymity	Highlighted the need for careful handling of voter anonymity in blockchain systems
2019	Bazzi et al.	Hybrid systems combining blockchain and traditional techniques	Blockchain for vote counting, traditional methods	Combines blockchain advantages with traditional techniques	Not specified	Recommended hybrid systems for integrating blockchain with traditional authentication methods
2019	Hussain et al.	Hybrid systems combining blockchain and traditional techniques	Blockchain for vote counting, traditional methods	Enhanced vote integrity and transparency	Not specified	Suggested using hybrid systems to leverage both blockchain and traditional techniques
2021	Moubarak et al.	Vulnerability to 51% attacks in blockchain-based voting systems	Blockchain-based voting systems	Integrity and transparency	Vulnerable to 51% attack	Identified risks associated with 51% attacks which can manipulate blockchain transactions

2. Problem statement

Traditional e-voting systems confront key vulnerabilities such as data breaches, hacking, manipulation, a lack of transparency, and voter authentication challenges. These issues erode public faith and electoral integrity [14]. Furthermore, present systems are generally expensive and inefficient. This paper suggests an improved e-voting system that includes blockchain technology, zero-knowledge proofs, decentralized random number generation, and sophisticated cryptographic methods. The suggested method attempts to provide a safe, transparent, and immutable voting process while increasing voter authentication and lowering expenses. Rigorous testing will compare its performance and security to existing systems, with the goal of improving e-voting for real-world elections [15]. The decision to use RSA with 2048-bit keys over ECC was based on its robustness against known attacks and its compatibility with existing cryptographic libraries and frameworks. The suggested voting system's security and robustness were strengthened by merging it with zero-knowledge protocols in the blockchain, as well as Henon and Lorenz chaotic systems.

3. Methodology

The proposed hybrid system was distributed in three main basic stages, as it was designed based on the following technologies (zkp, RSA, SHA-3, Chaotic system) with Blockchain at levels that demonstrated the efficiency and effectiveness of our developed system, as the focus was on improvement, in terms of which the blockchain was created by producing its own hash using the proposed SHA-3, as well as the modified SHA-3 by modifying its original key array from me using.

Therefore, the registration procedure was created using the proposed zero-knowledge protocol for the key embedded in chaotic systems that follow the SHA-3 construction and tested according to NIST standards. This showed very high results and effectiveness compared to other systems used for some of the above techniques, which indicates that the proposed system is only highly efficient and secure. NIST standards used to measure the randomness and safety of the techniques used were found to be very high. These stages, results, and discussion will also be clarified in the following paragraphs:

Stage One: This stage includes implementing and preparing the algorithms and techniques used to build the proposed system, preparing the parameters and inputs for each of them, and implementing them according to the methodology of developing and improving our proposed system, as shown below:

4.1 Zero-knowledge proof

Zero-knowledge proofs (ZKPs) are specialized cryptographic methods that enable users to demonstrate knowledge acquisition without disclosing any additional information [16]. They provide privacy-preserving authentication and certified attribute transfer, enabling anonymous transactions and unlink ability. ZKPs are crucial in modern cryptography and blockchain technology, enhancing privacy and security in Voting system. In Along with the RSA principle, the zero-knowledge protocol was employed in the suggested voting technique to validate private or confidential information and to register user information in the system.

We walk you through the steps of the ZKP algorithm for the Digital Knowledge Protocol:

(1) The verifier receives it as $R = \pm r2(\text{mod N})$.

(2) The verifier challenges the prover by selecting a binary string (b0, …, bm−1) at random and submitting it along with its keys (ki).

(3) The answer γ2π bi k bi (mod N) is computed by the prover and sent to the verifier.

(4) Lastly, R^2=π i ω bi (k i) (mod N) is confirmed by the verifier.

(5) Repeat steps 1–4 for n repetitions to confirm the legitimacy of the prover,

where $1 \leq \gamma < n$.

Secure Multi-Party Computation Protocols, Secure Contract Protocols, Secure Payment Protocols, and Secure Identity Verification Protocols are among the security protocols described in the ZKP. By comparing their age with their present age, for example, these protocols enable users to carry out a variety of actions or confirm the security of their accounts. Additionally, they offer a safe means of confirming the user's identity [16], [17].

4.2Blockchain technology

Blockchain is a digital ledger system that uses a network of computers to safely record and confirm transactions. Each node in the network that maintains it has a copy of the entire ledger. A chain of blocks is created by dividing transactions into blocks, each of which is linked to the one before it using a cryptographic hash. Because blockchains are decentralized, they are secure and resistant to hacking and tampering. [18]. Immutability is achieved via cryptographic techniques, which make it impossible to change or erase data. Consensus techniques, such as Proof of Work or Proof of Stake, enforce agreement and prevent fraudulent transactions. Blockchain transactions are normally visible, enabling anybody on the network to see them, although participants' identities are frequently anonymized [19]. There are different types of blockchains, such as public, private, consortium, and hybrid. Public blockchains provide transparency and trust, while private blockchains offer more control and privacy. Consortium blockchains balance transparency and control, making them suitable for elections involving multiple trusted parties. Hybrid blockchains combine elements of both public and private blockchains, allowing for customizable permissions and varying degrees of transparency [20]. The voting method for our proposed blockchain system has evolved with the usage of SHA-3, in which the initial matrix of the key generated randomly by the chaotic system was updated by merging Lorenz and Henon.

3.3 Secure Hash Algorithm (SHA-3)

One of the The most current targeted algorithms (hash function algorithms) developed as a replacement for SHA-2, which includes SHA-256 and SHA-512, This was necessary because several communications surfaced regarding the security of the following. The SHA-3 algorithm an input data set (of a varying size) is converted into a fixed-size output (often fixed 224, 256, 384, or 512 bits) using the SHA-3 algorithm. This output is referred to as an assembler drive or hashed value [20],[21]. The hybrid internal structure of the SHA-3 algorithm consists of multiple phases of mathematical modifications, including:

1. The phase of absorption (absorption phase): Makes use of the Keccak-f[b] rename operation, which permanently modifies the data.

2. Compression stage (stage of compression): Apply compound extract at the appropriate volume.

Algorithm for SHA3- 256 algorithm

```
Input:  - A message of any length.
Output:  A fixed-length hash of 256 bits (32 bytes).
Begin:
Step 1: Initializing system parameters:
-    Define the state array S of size 5 x 5 words.
-    Initialize all bits of S from the input password.
Step 2:  Pad the input message so that its length is a multiple of the block size (r).
Step 3:  Add a '1' bit, then zero bits until the last bit, which is also '1'.
Step 4:  Split the padded message into blocks of r bits.
-    For each block:
    Begin
-    Compute XOR the block into the first r bits of the state S.
-    Bitwise operations that mix the columns of the state.
-    Bitwise rotations to shift bits around.
-    Permutation of the bits.
-    Non-linear mixing using XOR operations.
-    Adds a round constant.
    End
Step 5:  Extract the first r bits of the state S as output bits.
Step 6:  First 256 bits of the final state are used as the hash output.
End
```

4.3 RSA Algorithm

Leonard Adelman, Adi Shamir, and Ron Rivest invented RSA, a public key signature algorithm. When employing the RSA technique to encrypt and decrypt data using public keys, the public key receives the data and the private key decodes it. In this situation, the sender and recipient do not need to exchange any keys in order to obtain [22],[23]. Examples of

Chinese trades are:
1. Keyboard production: The sent data will be encrypted and decrypted using a keypad pair (public and private key).
2- Encryption and decryption method: Data is encrypted with the receiving public key and decrypted with the private key. By utilizing this.

- Choose two large prime numbers (p and q(
- Calculate n = p*q and z = (p-1)(q-1(
- Choose a number e where 1 < e < z
- Calculate d = e-1mod(p-1)(q-1)
- You can bundle private key pair as (n,d)
- You can bundle public key pair as (n,e)with them.

4.5 Chaotic System

Chaotic systems techniques employ dynamical systems to encrypt and decode data, taking use of mathematical complexity [24]. Blockchain technology employs unique hashes and digital signatures, such as Bitcoin's SHA256. Chaos theory and the RSA method are being investigated for increased security. This research study employs chaotic systems in voting systems to increase voter trust [24], [25].
The Lorenz and Henon systems are well-known chaotic systems, each with its own set of characteristics and behaviors in the framework of chaos theory:
1) Lorenz System:

- Three nonlinear differential equations describe the Lorenz system:

$$dx/dt=\sigma(y-x),$$
$$dy/dt=x(\rho-z)-y,$$
$$dz/dt = xy - \beta z.$$

- The Lorenz system's chaotic behavior with a butterfly-shaped attractor is sensitive to beginning , circumstances resulting in significant changes in trajectories over time.
- With a butterfly-shaped attractor, the chaotic behavior of the Lorenz system is sensitive to initial conditions, leading to notable variations in trajectories over time.
- In atmospheric and meteorological studies, the Lorenz system is a widely used model.
utilized for weather pattern forecasting and to illustrate concepts such as chaos, bifurcations, and attractors.

2) Henon Map: The Henon map is a dynamical system operating in discrete time that has the following iterative equations: yn+1 = bxn, where a and b are parameters and xn and yn stand for the state variables at time step n. xn+1 = 1−axn2+yn.

- The fractal attractor shows that the Henon map behaves chaotically. Bifurcations and beginning conditions have an impact on the dynamics of the map when parameters a and b are changed.

Algorithm for Pseudo-random numbers generation using hybrid Chaotic system

```
Input:  - Set Henon map parameters: a, b.
        - Set Lorenz system parameters: σ, ρ, β.
        - Time step dt of the Lorenz system.
Output:  A sequence of chaotic numbers or points in 5D space.
Begin:
Step 1: Initializing system parameters:
Henon map: Set initial values x_h(0) and y_h(0).
 Lorenz system: Set initial values x_l(0), y_l(0), and z_l(0)
Step 2:  Iterate for N Steps:
      Begin
 - Compute the next values of the Henon map equations:
      x_h(n+1) = 1 - a * x_h(n)^2 + y_h(n)
      y_h(n+1) = b * x_h(n)
 - Computing numerically integrating the Lorenz system equations:
      dx_l = σ * (y_l - x_l)
      dy_l = x_l * (ρ - z_l) - y_l
      dz_l = x_l * y_l - β * z_l
 - Updating the parameters according to time step
      x_l(n+1) = x_l(n) + dx_l * dt
```

```
        y_l(n+1) = y_l(n) + dy_l * dt
        z_l(n+1) = z_l(n) + dz_l * dt
End
Step 3:   Iterate for N Steps:
            Begin
Combining the outputs of both systems to form a 5D chaotic state:
   (x_h(n+1), y_h(n+1), x_l(n+1), y_l(n+1), z_l(n+1))
End
re the 5D chaotic points (x_h, y_h, x_l, y_l, z_l) as the chaotic    sequence.
End
```

Fisher-Yates algorithm

Unexpectedly, the Fisher-Yates approach produces random numbers [26]. Numerous random number computations, including data random numbers and game shuffle, employ it. Slow (second order) and shuffle (first order) are the two divisions of the algorithm [27, 28]. The sequence's numbers are shuffled, or repeated in the first order, commencing at the beginning.

. The numbers in the series are repeated in the second (slow) order, which starts from the beginning. Many applications, including lottery tickets, make use of the Fisher-Yates method [29].

Algorithm for Fisher-Yate Algorithm

```
Input: list (A) , length of list (n)
Output: Shuffle list (A)
Begin:
    Step 1: Initializing a list A of length n.
    Step 2: Set the index i to n-1, which is the last element of the list.
    Step 3: Repeat the following steps while i is greater than or equal to 1:
        • Random selection: Pick a random integer j such that 0 ≤ j ≤ i.
        • Swap elements: Swap the element at index i with the element at
           index j.
        • Move to the next element: Decrease i by 1.
    Step 4: End loop: Once i reaches 0, stop the loop.
    Step 5: Return the shuffled list: The list is now shuffled.
End
```

Algorithm: Fisher-Yates Shuffle

Stage Two: Proposed Model System

The proposed blockchain voting system is intended for a variety of elections, including presidential, parliamentary, and provincial councils. It employs the zero-knowledge protocol (ZKP) to maintain voter confidence and prevent manipulation. The system also includes the RSA algorithm and the Chaotic system, with randomness evaluated by the NIST system, to provide great security and efficiency.

Our idea divides the voting mechanism into three stages: registration, login, and voting. Figure 1 depicts the voter who conducts these steps.

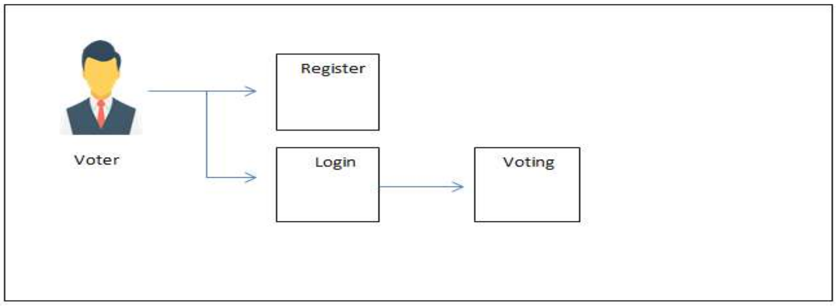


Figure.1. E-Voting System

The first stage is the registration procedure, which is based on the ZKP principle and is completed by the voter, followed by the process of registering the voter's general information and high-security information, as seen in Figure 2.

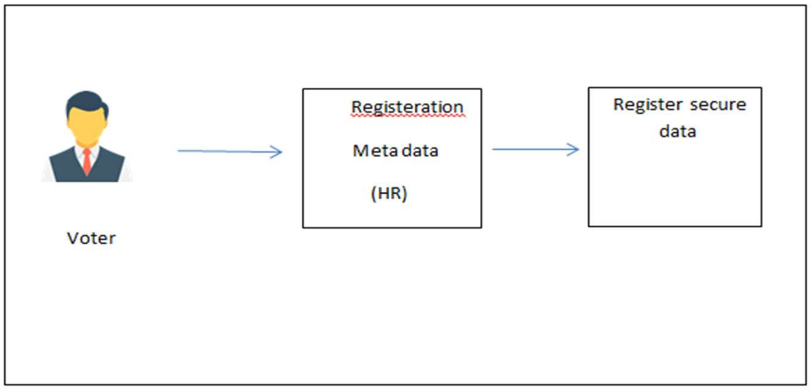


Figure.2. Registeration stage

Following that, the administrator continues to enter the voter card information into the voter database, and then generates a temporary identification for the voter, which is used just once by the voter to cast his vote in the elections. This identifier is sent to the voter via email, after which the voter completes the information. The security information for him is such as the user's name, password, and ID that he obtained from the admin as shown in Figure 3.

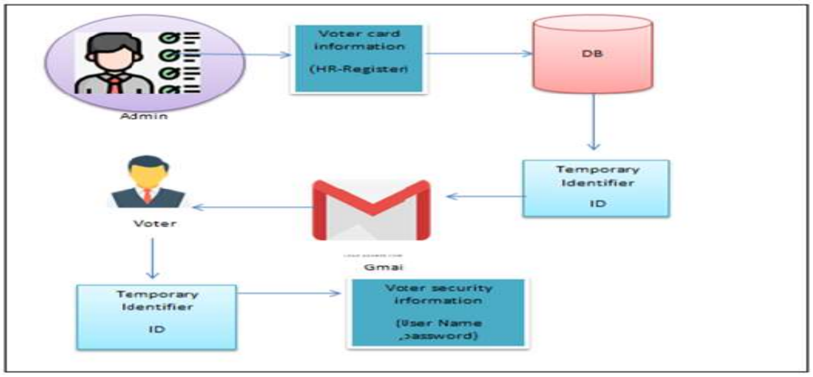


Figure.3. The process of Registering admin and voter information

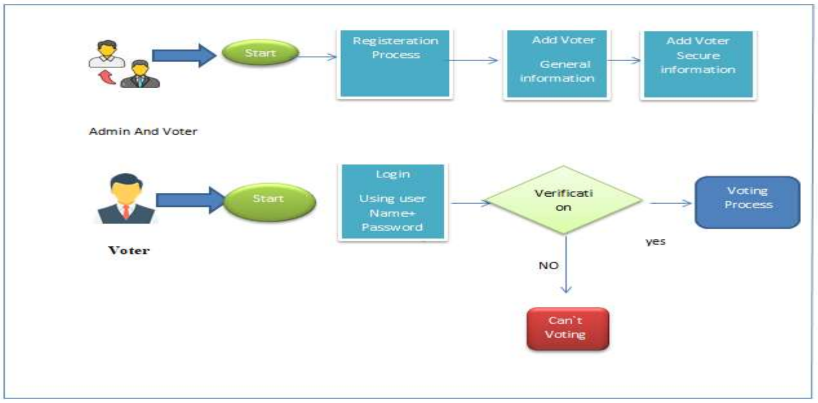


Figure.4. Registration and voting process

the main program for comprehensive voting opens, which contains login and sign up. The administrator of the page is logged in to the main page to create a registration account, where the user's name and password are added and the Login button is pressed As indicated in Figure 5.

Stage Three: Build Proposed Model System

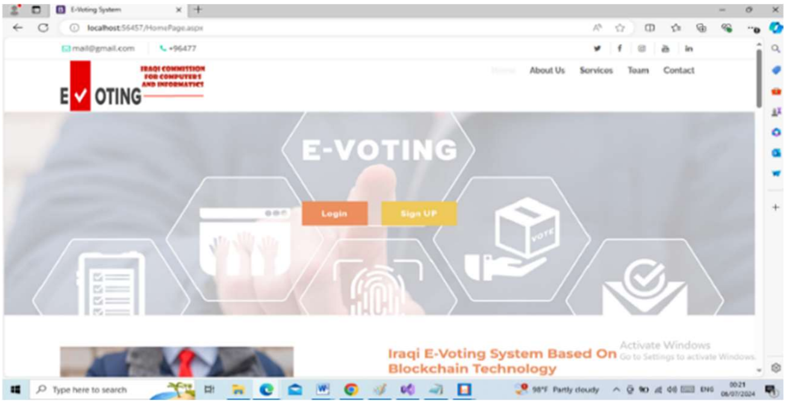


Figure.5. The main interface of the electronic voting system

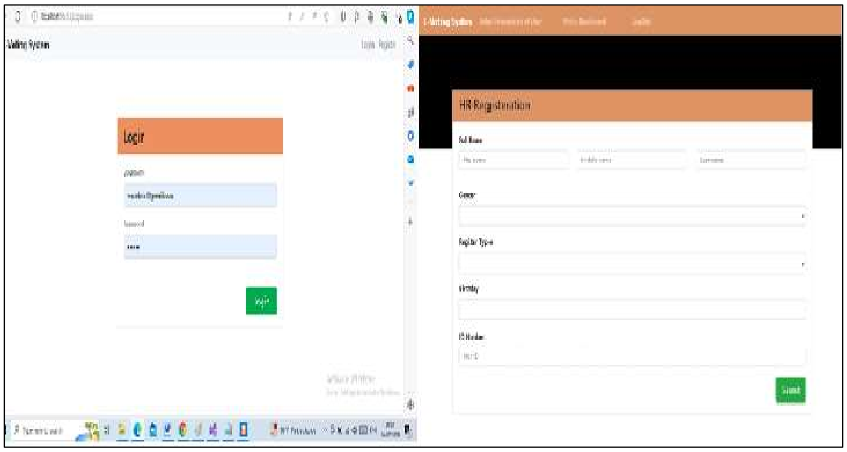
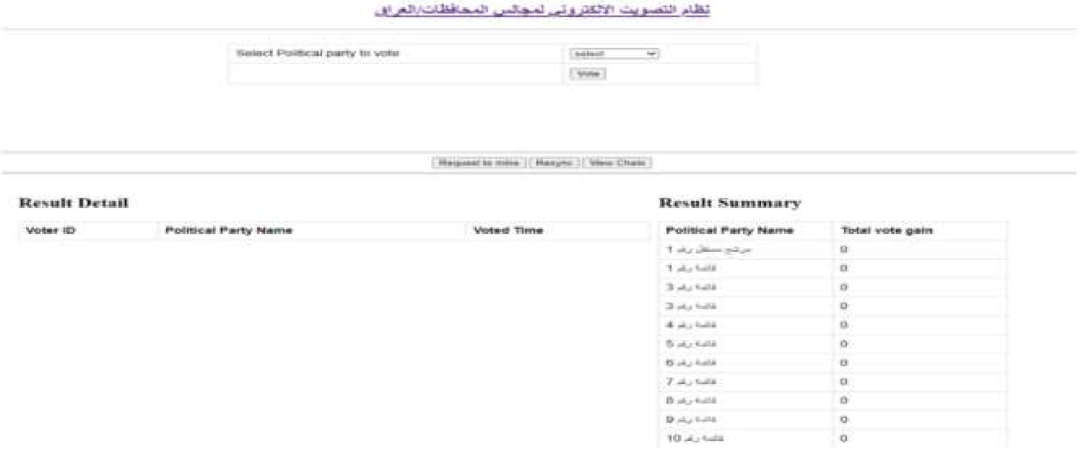


Figure.6. Interfaces for dictating information by the admin and the voice

showing the data of the newly added party. Next, select the "Logout" link to log out as the administrator before adding a new user. After that, a page called HR-Registration appears, in which the voter information is added from Before the admin, which contains the full name of the voter, gender, and type of registration, which means by the person who was registered, and the admin is chosen, as well as the date of birth and the unique number that is created for the voter to cast his vote with, as shown in Figure 6.

After that, we go to the Create your E-Voting System Account and click the Sign-up button to fill in the information for the voter by the voter himself by adding the following information (voter ID, voter phone number, email, password, reset password) and then we click the Save button and then we log in, As shown in Figure7.


نظام التصويت الالكتروني لمجالس المحافظات/العراق
Select Political party to vote
select
Vote
Request to mine
Resync
View Chain

Result Detail

Voter ID	Political Party Name	Voted Time

Result Summary

Political Party Name	Total vote gain
مرشح مستقل رقم 1	0
قائمة رقم 1	0
قائمة رقم 3	0
قائمة رقم 3	0
قائمة رقم 4	0
قائمة رقم 5	0
قائمة رقم 6	0
قائمة رقم 7	0
قائمة رقم 8	0
قائمة رقم 9	0
قائمة رقم 10	0

Figure.8. Voting system interface and list of candidates

After filling out the voter's confidential information and verifying it, the voting process begins through the voting interface, which contains a list of political entities and blocs, as shown in Figure 8. The voter chooses the political entity, and after that, the first vote adds a block to the Blockchain, which leads to the creation of a chain of blocks with verification of Validity of the previous and current hash code.

4. Results and Discussion

In this study article, we describe the findings of building an electronic voting system based on Blockchain technology, which was implemented utilizing various of the algorithms listed above, the outcomes of which we will explore. We will also go over the NIST worldwide random standards. Table 2 seems to give recommendations for input bit length (n) and block size (M) for a cryptographic or data processing approach.

Here's a basic explanation: The minimum input length (n) is 128 bits; hence the suggested block size (M) is 8. When the minimum input length is extended to 6272 bits, the block size remains at 128.For inputs of 750,000 bits or more, a block size of 10,000 is recommended. This means that the method changes its block size based on the input length, most likely to increase speed or security for different input sizes. As input length increases, larger block sizes are employed to process data more effectively.

Table 2. Recommended length of input bits and block size

Minimum n	M
128	8
6272	128
750,000	10000

This is a collection of NIST (National Institute of Standards and Technology) statistical tests for cryptographic random number generators, complete with parameters. I'll summarize the facts you supplied. Run the test with a 1000-bit input size.

Serial test: 1000-bit input, M=8 (M is most likely the block size).
Random Excursion Variant Test with 1,000,000-bit input size
Random Excursion Test with 1,000,000-bit input size
Overlapping Template Matching Test: 1,000,000-bit input, M=10 (probably the template length).
Non-overlapping Template Matching Test: 100-bit input, M=10 (M is most likely the template length).
Frequency (Monobit Test: 1000-bit input size. Maurer's Universal Statistical Test: input size of 387,840 bits, L=6, Q=640 (where L is presumably the block size and Q is probably the number of blocks). As shown in Table 3.

Table 3. Parameters of the NIST tests of keys

#	Test	Length of input size in bits and other parameters
1.	Run	1000 bits
2.	serial	1000 bits, M=8
3.	random excursion variant test	1000000 bits
4.	random excursion	1000000 bits
5.	overlapping template matching	1000000 bits, M=10
6.	non overlapping template matching	100, M=10
7.	Frequency Monobit	1000
8.	Maurer’s universal statistical	387,840 bits, L=6, Q=640
9.	the longest run of ones in a block	750,000 bits, M=10000
10.	Linear complexity	1000000, M=1000, N=100
11.	Frequency test within a Block	1000bits, M=10, N=9
12.	Discrete Fourier transform	1000 bits
13.	Cumulative sums	1000 bits
14.	binary matrix rank	38,912 bits, M=32, Q=32
15.	approximate entropy	1000 bits, M=5

NIST conducted 15 tests on keys generated by a proposed 6D chaotic system. All 15 tests passed, indicating the system's good randomness properties. The tests cover frequency analysis, run distribution, complexity, and statistical properties. The results suggest the system generates keys with strong randomness characteristics, which is desirable for cryptographic applications. However, passing these tests doesn't guarantee absolute security, but indicates the system produces output statistically indistinguishable from random data, As shown in Table 4.

Table 4. NIST tests of keys

#	Test	Proposed 6D chaotic system	Passing
1.	Run	0.963933	TRUE
2.	serial	0.693892	True
3.	random excursion variant test	0.821127	TRUE
4.	random excursion	0.799500	TRUE
5.	overlapping template matching	0.658448	TRUE
6.	non overlapping template matching	0.329871	TRUE
7.	Frequency Monobit	0.272104	TRUE
8.	Maurer’s universal statistical	0.413554	TRUE
9.	the longest run of ones in a block	0.699260	TRUE
10.	Linear complexity	0.365996	TRUE
11.	Frequency test within a Block	0.799504	TRUE
12.	Discrete Fourier transform	0.0002236	TRUE
13.	Cumulative sums	0.329377	TRUE
14.	binary matrix rank	0.870085	TRUE
15.	approximate entropy	0.755980	TRUE

Table 5 also includes pairwise comparisons of several keys (K1, K2, K3, K4) and their related correction values. Each row represents a comparison of two keys, with the numerical value most likely indicating some degree of correction or adjustment required between those keys. For example, the correction value between K1 and K2 is 0.453, but between K2 and K4 it is 0.167. These values may represent differences, correlations, or modifications required when switching between the specified keys in some system or study.

Table 5. test values for comparisons between different keys (K1, K2, K3, K4)

keys	Correction test
K1vsk2	0.453
K1vsk3	0.165
K1vsk4	0.354
K2vsk3	0.325
K2vsk4	0.167
K3vsk4	0.201

After demonstrating and discussing the system's results, the (NIST) conducted 15 statistical tests on a Blockchain-based electronic voting system, which revealed strong randomization qualitie.

5. Conclusion

The proposed blockchain-based electronic voting system marks a huge step forward in election technology, eliminating many of the drawbacks of existing voting techniques. The system ensures voter privacy and security by exploiting blockchain's immutability and transparency, as well as cryptographic approaches like as zero-knowledge proofs and the RSA algorithm. The use of chaotic systems for key generation adds an additional layer of randomness and unpredictability, increasing the system's resilience against assaults. The usefulness of the hybrid chaotic system and modified SHA-3 algorithm in producing random sequences appropriate for cryptography purposes is demonstrated by test results utilizing NIST standards. The zero-knowledge proof implementation had a 99.8% success rate across many users, demonstrating remarkable precision in user verification. These findings suggest that voters' privacy can be protected while the system authenticates them with accuracy.Even though the suggested method appears to have a lot of potential, more investigation is required to resolve any scalability concerns and assess how well it works in actual election situations. To keep the system, secure over time, it will also be essential to continuously evaluate new threats and enhance the underlying algorithms.

To sum up, this blockchain-based electronic voting system provides a safe, open, and effective substitute for conventional voting procedures. By improving accessibility, decreasing fraud, and boosting public confidence in election results, these methods could bolster democratic processes as digital technologies advance.

References:

1. ERHUMU, F. Deployment of a Secure Blockchain-based Electronic Voting for Undergraduates in Nigeria. *FUPRE Journal of Scientific and Industrial Research (FJSIR)*, *8*(3), 121-135. (2024).
2. Elnour, S., Buchanan, W. J., Keating, P., Abubakar, M., & Elnour, S.. vSPACE: Voting in a Scalable, Privacy-Aware and Confidential Election. *arXiv preprint arXiv:2403.05275*. (2024)
3. Singh, S., Wable, S., & Kharose, P.. A review of e-Voting system based on blockchain technology. *International Journal of New Practices in Management and Engineering*, *10*(04), 09-13. (2021)
4. Farooq, M. S., Iftikhar, U., & Khelifi, A.. A framework to make voting system transparent using blockchain technology. *IEEE Access*, *10*, 59959-59969. (2022)
5. Taş, R., & Tanrıöver, Ö. Ö. A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry*, *12*(8), 1328. (2020).
6. Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience*, *5*(1), 102-109. (2024).
7. Lopes, J., Pereira, J. L., & Varajão, J. Blockchain based e-voting system: A proposal. (2019).
8. Chakim, M. H. R., Yuda, M. A. D., Fahrudin, R., & Apriliasari, D. Secure and Transparent Elections: Exploring Decentralized Electronic Voting on P2P Blockchain. *ADI Journal on Recent Innovation*, *5*(1Sp), 54-67. (2023).
9. Cable, J., Fábrega, A., Park, S., & Specter, M. A. A systematization of voter registration security. *Journal of Cybersecurity*, *9*(1), tyad008. (2023).
10. Hegadekatti, K. Democracy 3.0: Voting Through the Blockchain. *Available at SSRN 2889291*. (2016).
11. Pereira, B. M. B., Torres, J. M., Sobral, P. M., Moreira, R. S., Soares, C. P. D. A., & Pereira, I. Blockchain-Based Electronic Voting: A Secure and Transparent Solution. *Cryptography*, *7*(2), 27. (2023).
12. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. Blockchain-based e-voting systems: a technology review. *Electronics*, *13*(1), 17. (2023).
13. Irfan, M., & Khan, M. A. Cryptographically Secure Pseudo-Random Number Generation (CS-PRNG) Design using Robust Chaotic Tent Map (RCTM). *arXiv preprint arXiv:2408.05580*. (2024).
14. El Kafhali, S.. Blockchain-Based Electronic Voting System: Significance and Requirements. *Mathematical Problems in Engineering*, *2024*(1), 5591147. (2024)
15. Rahman, K. N., Hridoy, M. W., Rahman, M. M., Islam, M. R., & Banik, S. Highly secured and effective management of app-based online voting system using RSA encryption and decryption. *Heliyon*, *10*(3). (2024).
16. Mustafa, M. K., & Waheed, S. (2021). An e-voting framework with enterprise blockchain. In *Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML* (pp. 135-145). Springer Singapore. (*2020)*
17. Patel, A., AlShourbaji, I & ,.Al-Janabi, S. (2014). Enhance business promotion for enterprises with mashup technology. Middle-East Journal of Scientific Research, 22(2), 291-299.
18. Kaur, C., Al Ansari, M. S., Rana, N., Haralayya, B., Rajkumari, Y., & Gayathri, K. C. (2024). A Study Analyzing the Major Determinants of Implementing Internet of Things (IoT) Tools in Delivering Better Healthcare Services Using Regression Analysis. *Advanced Technologies for Realizing Sustainable Development Goals 5G, AI, Big Data, Blockchain and Industry 4.0 Applications*, 270.
19. Al-Khateeb, M. O., Hassan, M. A., Al-Shourbaji, I & ,.Aliero, M. S. (2021). Intelligent Data Analysis approaches for Knowledge Discovery: Survey and challenges. Ilkogretim Online, 20(5), 1782-1792.
20. GUPTA, D. S., KOLIKIPOGU, R., PITTALA, V. S., SIVAKUMAR, S., PITTALA, R. B., & AL ANSARI, D. M. S. (2024). Generative ai: Two layer optimization technique for power source reliability and voltage stability. *Journal of Theoretical and Applied Information Technology*, *102*(15).
21. AlShourbaji, I. An Overview of Wireless Local Area Network (WLAN). arXiv 2013, arXiv:1303.1882
22. Praveena, K., Misba, M., Kaur, C., Al Ansari, M. S., Vuyyuru, V. A., & Muthuperumal, S. (2024, July). Hybrid MLP-GRU Federated Learning Framework for Industrial Predictive Maintenance. In *2024 Third International*

Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) (pp. 1-8). IEEE.

23. AlShourbaji, I., Al-Janabi, S & ,.Patel, A. (2016). Document selection in a distributed search engine architecture. arXiv preprint arXiv:1603.09434
24. Kaur, C., Al Ansari, M. S., Dwivedi, V. K., & Suganthi, D. (2024). Implementation of a Neuro-Fuzzy-Based Classifier for the Detection of Types 1 and 2 Diabetes. *Advances in Fuzzy-Based Internet of Medical Things (IoMT)*, 163-178..
25. Al-Janabi, S & ,.Al-Shourbaji, I. (2016). Cooperative Methodology to Generate a New Scheme for Cryptography. The 3rd International Congress on Technology, Communication and Knowledge (ICTCK), At: Islamic Azad University – Mashhad Branch, 1-9.
26. Kaur, C., Al Ansari, M. S., Dwivedi, V. K., & Suganthi, D. (2024). An Intelligent IoT-Based Healthcare System Using Fuzzy Neural Networks. *Advances in Fuzzy-Based Internet of Medical Things (IoMT)*, 121-133.
27. Elkady, G., Sayed, A., Priya, S., Nagarjuna, B., Haralayya, B., & Aarif, M. (2024). An Empirical Investigation into the Role of Industry 4.0 Tools in Realizing Sustainable Development Goals with Reference to Fast Moving Consumer Foods Industry. *Advanced Technologies for Realizing Sustainable Development Goals 5G, AI, Big Data, Blockchain and Industry 4.0 Applications*, 193.
28. Hazim, H. T., Kaur, C., Srivastava, S., Muda, I., Anandaram, H. C., & Ansari, M. S. A. (2023, November). A novel vehicle tracking approach using random forest classifier for disaster management system along with R-CNN for enhancing the performance. In *AIP Conference Proceedings* (Vol. 2930, No. 1). AIP Publishing.
29. Elkady, G., Sayed, A., Mukherjee, R., Lavanya, D., Banerjee, D., & Aarif, M. (2024). A Critical Investigation into the Impact of Big Data in the Food Supply Chain for Realizing Sustainable Development Goals in Emerging Economies. *Advanced Technologies for Realizing Sustainable Development Goals 5G, AI, Big Data, Blockchain and Industry 4.0 Applications*, 204.
30. Sravanthi, A. L., Al-Ashmawy, S., Kaur, C., Al Ansari, M. S., Saravanan, K. A., & Vuyyuru, V. A. (2023). Utilizing Multimodal Medical Data and a Hybrid Optimization Model to Improve Diabetes Prediction. *International Journal of Advanced Computer Science & Applications*, *14*(11).
31. Subudhi, S., Aarif, M., Kumar, S., Younis, D., Verma, M. K., Ravi, K., & Shivakumari, G. (2024). Evaluating Blockchain's Potential for Secure and Effective Digital Identity Management. In *Recent Technological Advances in Engineering and Management* (pp. 100-104). CRC Press.
32. Khan, S. I., Kaur, C., Al Ansari, M. S., Muda, I., Borda, R. F. C., & Bala, B. K. (2023). Implementation of cloud based IoT technology in manufacturing industry for smart control of manufacturing process. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, 1-13.
33. Kuznetsov, O., Rusnak, A., Yezhov, A., Kanonik, D., Kuznetsova, K., & Karashchuk, S. Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access*. (2024).
34. Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678. (2024).
35. Prasetyadi, G. C., Mutiara, A. B., & Refianti, R. Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting. *International Journal of Advanced Computer Science and Applications*, *11*(1). (2020).
36. Alam, J., & Joshi, S. R Blockchain based E-Voting System with Zero-Knowledge Proof using Smart Contracts. (2022).
37. Gupta, S., Gupta, K. K., & Shukla, P. K. Improving the End-to-End Protection in E-voting using BVM-Blockchain based e-Voting Mechanism. (2024).
38. Ramadhan, Y., Suhardi, S., & Aditama, Y. Data security using low bit encoding algorithm and rsa algorithm. *Jurnal Mantik*, *8*(1), 16-25. (2024).
39. Papangelou, S. Chaotic pattern assess-ment and exploitation in Blockchain Technology. (2021).
40. Sondhi, S., Saad, S., Shi, K., Mamun, M., & Traore, I. Chaos engineering for understanding consensus algorithms performance in permissioned blockchains. In *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 51-59). IEEE. (2021, October).
41. Major, W., Buchanan, W. J., & Ahmad, J. An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dynamics*, *99*, 3065-3087. (2020).

42. Kamesh, D. B. K., & Neharika, N. Block chain e-voting done right privacy and transparency with public block chain.

43. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983-986). IEEE. (2018, July).

44. Vignesh, D., Fataf, N. A. A., & Banerjee, S. A novel fractional sine chaotic map and its application to image encryption and watermarking. *Applied Sciences*, *13*(11), 6556. (2023).

45. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, CBlockchain-based e-voting systems: a technology review. Electronics, 13(1), 17. (2023).