Journal of Soft Computing and Computer Applications

Volume 2 | Issue 1 Article 1018

2025

Blockchain-based Physical Election Votes Digitally Secure Transfer

Mohanad A. Mohammed
General Company for Air Navigation Services (GCANS), Baghdad International Airport, 3rd Floor Baghdad, Iraq, mohanadalimm@gmail.com

Hala B. Abdul Wahab
University of Technology, Department of Computer Science, Al-Sina'a St., Al-Wehda District, 10066 Baghdad, Iraq, hala.b.abdulwahab@uotechnology.edu

Recommended Citation

Mohammed, Mohanad A. and Wahab, Hala B. Abdul (2025) "Blockchain-based Physical Election Votes Digitally Secure Transfer," *Journal of Soft Computing and Computer Applications*: Vol. 2: Iss. 1, Article 1018.
DOI: https://doi.org/10.70403/3008-1084.1018

JOURNAL OF SOFT COMPUTING AND COMPUTER APPLICATIONS 2025;2:1018

ORIGINAL STUDY

Blockchain-based Physical Election Votes Digitally Secure Transfer

Mohanad A. Mohammed [a,*], **Hala B. Abdul Wahab** [b]

[a] General Company for Air Navigation Services (GCANS), Baghdad International Airport, 3rd Floor Baghdad, Iraq
[b] University of Technology, Department of Computer Science, Al-Sina'a St., Al-Wehda District, 10066 Baghdad, Iraq

ABSTRACT

Responsibility for maintaining election transparency over time and ensuring democratic values intact is held by the Iraqi Independent High Electoral Commission (IHEC). However, transferring physical election votes from election centers is a critical duty, where many challenges appear regarding accountability and security measures. This study proposes a system that utilizes blockchain technology to solve any challenges or difficulties and ensure an effective and improved election process by providing its highest trustworthiness and legitimacy and ensuring a decentralized security process. This system offers unique blockchain characteristics such as immutability, decentralization, and transparency, providing an extra level of security to the data against fraud attacks and providing anti-tamper. This system includes three main components: the first includes Internet of Things (IoT) scanners for election centers, which are responsible for saving physical voting results encrypted using homomorphic encryption algorithms. The second includes IHEC servers, which collect votes from multiple election centers and verify the authenticity of each one. The third is blockchain, which is used to securely transfer votes between these two components to ensure transparency and accountability that voters have voted and that no vote can be altered without being detected. As a result, the proposed system efficiently utilizes a lightweight private blockchain, Proof of Secret Sharing (PoSS) consensus. Compared to blockchain systems, it shows faster Transaction Per Second (TPS) of 37.84%, 84.14% in verification time, 87.39% in the final time, CPU usage of 73.94%, and CPU user time of 0.29%.

Keywords: Elections, Physical voting, Blockchain, Consensus mechanism

1. Introduction

The new world is where new technologies merge with old concepts and values, such as merging democracy and technology, where technology is mainly used to ensure an effective, safe, and fair election. In Iraq after 2003, and like in other countries worldwide,

Received 15 March 2024; revised 25 May 2025; accepted 26 May 2025.
Available online 14 June 2025

* Corresponding author.
E-mail addresses: mohanadalimm@gmail.com (M. A. Mohammed), hala.b.abdulwahab@uotechnology.edu (H. B. Abdul Wahab).

https://doi.org/10.70403/3008-1084.1018

the election process is considered a pillar of democratic governance. It is used to let the authorities and the people ensure that people's votes are respected and heard, and it also affects the political field. However, the process of transferring physical election votes from different election centers to the Iraqi Independent High Electoral Commission (IHEC) servers reflects many challenges related to authentication and tamping [1].

Without accurate and effective votes of electors, there is no democracy since citizens' votes reflect their preferences and elect representatives about the whole country's future. Maintaining the authenticity, accuracy, and confidentiality of these votes is considered a recent challenge. Blockchain is considered a trend and effective solution to these upcoming challenges and offers a new paradigm of trust in the digital age [2].

Blockchain technology, by its nature, provides an immutable and decentralized nature of the system, which means ensuring the people's vote integrity. Since the elector's role ends up with the physical paper and his vote, the journey of his votes starts with the blockchain parts and finally ends in the unchangeable digital ledger, which can be tracked and verified continuously. The cryptographic algorithm inside the blockchain, specifically the hash, guarantees that once a vote is recorded, it will then be immune to manipulation or tampering, bolstering the security of the electoral process.

After the voter and the automatic reader have made the vote registers, the vote is saved in a tamper-evident container, and those devices generate unique QR codes that link them to the blockchain. The accuracy of each vote cast in the election, consequently, is paramount and creates digital fingerprints. Using scanning and registration in the election centers, consensus mechanisms are used in propagating these digital fingerprints across the blockchain peer-to-peer network currently used within most blockchains, resulting in trustworthiness among everyone involved [3].

When the IHEC servers receive the updated list of votes, they verify it by comparing the scanned votes with their digital fingerprints on the blockchain, thus ensuring that all votes are accurate and authentic.

This process offers many advantages, such as transparency for the election observers, political parties, and any other interested party to access this information on the blockchain network. It also allows trust and reduces vote fraud in the election process [4].

Using blockchain to physically transfer election votes in Iraq presents significant benefits, but also raises more challenges that need to be considered for a successful implementation. These challenges relate to infrastructure, technical know-how, and collaboration among stakeholders.

This study proposes a basic system for blockchain-based physical election votes digitally secure transfer. It takes into account the expected difficulties, technical, and implementation considerations, and accepts technology alongside the advantages of adopting blockchain. This will enhance transparency and integrity while ultimately building citizen trust within democratic systems.

The main challenges in implementing the proposed blockchain-based voting system include ensuring authentication to prevent unauthorized access, maintaining the integrity and confidentiality of votes, achieving scalability to handle a high volume of votes, and overcoming infrastructure limitations in regions like Iraq. Additionally, technical challenges such as training personnel in blockchain technology and fostering collaboration among voters, election authorities, and observers are critical to the system's success.

The main contribution of this study is to propose a secure, decentralized election vote transfer system using a lightweight private blockchain with PoSS consensus, integrating IoT scanners and homomorphic encryption to enhance transparency, security, and performance compared to traditional election solutions.

This study is organized as follows: the traditional election system is explained in Section 2, the related work is presented in Section 3, and how to use the blockchain in elections is shown in Section 4. The proposed system and its implementation are explained step by step in Section 5 and Section 6, respectively. The results are shown in Section 7, and the discussion is presented in Section 8. Finally, the conclusion is presented in Section 9.

2. Traditional election system

People have been participating in the election process for a long time, which is the traditional voting system, followed by the process of casting the votes and counting them. Election centers usually receive a huge amount of people exercising their democratic rights, with hopes and wishes for the future of their local communities through this process.

During special dates set by the IHEC in countries where elections are taking place, voters have to provide valid identity details before participating in the election process, receiving the election special paper, and making decisions privately in specified booths. When these dates end, election officials gather the election boxes from the election centers, and authorized employees start the hours-long marathon counting sessions to finalize the results with extra caution for all small details or any votes which could affect the final result [5].

Even though this system has been used for decades in the democratic processes, it still has many negative sides to be considered and treated, as manual tallying of election stations has different and logistic hurdles that arise when transporting vote boxes from election centers' locations to centralized collection points. Besides the real-time challenges and transparency concerns, since only a pre-determined number of people can watch the counting process, there may sometimes be concerns or doubts about the accuracy or integrity of the results [6].

For decades, the system used for election was considered a great and successful tool in democratic decision-making and a good mirror for reflecting people's opinions and hopes regarding the political and election systems. However, recent times have brought the use of new technology such as blockchain, which appears to be helping election systems but also adding new challenges, reflecting the potential to change the shape of modern election systems in many countries [7].

3. Related work

Many studies and research discussed the possibilities for transition from traditional voting systems to electronic voting systems and online voting systems. The following studies show the challenges, benefits, and technological advancements required for such a transition in Iraq and applying the e-voting within the country.

The authors in [8] presented a comprehensive analysis of the traditional voting system and how to transition from such a system to the online voting system in Iraq. The study reflected many challenges related to the current election situation in Iraq such as security vulnerabilities and inefficiencies. The authors, after discussing the whole scenario, recommended transitioning from a traditional to an online voting system. This transition would provide benefits such as increased accessibility for the elderly and disabled voters and enhanced trust and security for both users and the government.

New research focused on the integration of blockchain in e-voting systems has been presented in [9]. The authors explored this issue to enhance trust while keeping transparency at the highest levels. Since the current consensus algorithm in blockchain is not

suitable for use in an election system, because it consumes a huge amount of power and computational resources, a novel consensus algorithm was proposed for such purpose known as PSC-Bchain. This algorithm combines Proof of Credibility and Proof of Stake to improve the efficiency and security of blockchain-based voting, employing it with the smart contracts helps in establishing a reliable public bulletin board while keeping the system capable of scalability and security.

The authors in [10] proposed a model for e-voting in Iraq. While they discussed the challenges related to such a type of voting, they also focused mainly on the design and testing of such a system and tried to measure its level of security compared to the paper-based elections. The system consists of a user-friendly, reliable, and simple platform, as well as a secure system for the online voting process that employs credentials for verification, aiming to increase participation and address common voting challenges in Iraq.

The authors in [11] suggested trust as a mediation to adopt the electronic voting system in Iraq. The authors employed the concept of using the role of trust as a main factor for electronic voting system adaptation. In this system, the main impact on the election process is discussed while identifying the main factors affecting its use such as security, privacy, usability, and reliability. The authors used a survey of 299 respondents, and the study revealed significant positive relationships between trust and these factors, offering valuable insights for the Iraqi government to replace paper-based systems with efficient e-voting solutions.

The authors in [12] proposed a system for e-voting that employs the web as a platform and replaces the paper-based voting system and manual counting for the votes which may lead to some counting errors and the risk of obsolete votes. This platform was programmed using ASP.NET and SQL Server. The authors also discussed how such a system offers numerous benefits, including time savings, reduced counting errors, and more.

The authors in [13] built on the previous system, where authors developed a web-based voting system that employs Ethereum building Ethereum-based e-voting DApp. This platform was programmed using ASP.NET and SQL Server as a front-end to improve accessibility. By addressing common issues such as vote manipulation and system transparency, blockchain-powered e-voting solutions have the potential to provide a fair, verifiable, and fully decentralized election process while maintaining voter anonymity.

A blockchain-based electronic voting system leveraging smart contracts to enhance security and transparency has been proposed by the authors in [14]. The work, presented at AITC-2023 and CSSP-2023, demonstrates how Ethereum's decentralized architecture can be utilized to ensure vote integrity and anonymity, reducing the risk of election fraud.

The above studies collectively underline the growing interest in adopting electronic and online voting systems in Iraq. However, these studies predominantly focus on conventional Internet and mobile-based technologies. The current study aims to address the gap by introducing a blockchain-based framework for securing votes of traditional voting, leveraging the inherent security, transparency, and immutability of blockchain technology to provide a robust and trustworthy solution tailored to Iraq's unique socio-political landscape.

4. Blockchains in the election

Nowadays, blockchain technology, through specialists, plays a transformative role within the voting and election system worldwide and brings a revolutionary way for voters to realize and act with the democratic processes. Trust, transparency, and security are the pivots of how the electoral systems stand. Blockchain offers the potential to realize this vision, bringing about a paradigm shift in how votes are cast, counted, and verified [15].

Blockchain technology provides a distributed digital ledger that stores the transaction (information) in a decentralized environment and offers immutable characteristics, which make it the best choice for improving transparency and integrity in the voting and election systems.

The anti-tampering capability of the blockchain can be a huge benefit to the voting process since the voting record cannot be deleted, edited, or altered. Each vote is registered successfully and securely recorded within the ledger as a block, which, together with other votes or blocks, makes a chain of blocks called a blockchain, chronologically storing the voting data. Once recorded on the blockchain, it becomes nearly impossible to manipulate or modify without network consensus, ensuring electoral process integrity [15].

Since blockchain is a decentralized system by its nature, any votes or records within the blockchain can be verified. They can also be known by the owner and viewed by anyone within the network with transparent access, including election observers, political parties, media, and citizens themselves. This reflects the transparency potential of blockchain. Accordingly, individuals can independently audit the voting process to ensure fairness and legitimacy [16].

Blockchain offers many cryptographic algorithms that provide extra benefits regarding security and privacy concerns. Votes are not saved as plaintext within the blockchain but are encrypted and kept confidential through this technology use, reducing the risk of unauthorized access or manipulation, as there is no central authority vulnerable to hacking or tampering. Furthermore, blockchain offers great auditability and verifiability for the votes using a digital signature, which is unique and private for all votes saved within the blockchain [17]. Table 1 shows traditional and blockchain-based comparisons [18].

The traditional election process allows each person to use his right to vote, but it still requires that he visit the election center and the specially designed voting stations. He can cast his vote using paper ballots—ensuring confidentiality around their choices made publicly available through manually handling collected ballot papers that are eventually stored inside sealed containers, fostering high-integrity polls with stringent security measures around them. This system still faces some problems regarding intentional or unintentional errors, and human surveillance errors, which affect the accuracy of the declared election results [19].

When compared to the voting system that is based on blockchain, many benefits are reflected in the election process, such as efficiency and reliability. Although voters still need to physically visit the election centers for their votes instead of relying on classical and manual steps starting from data collection, storing, and ending with transparency-checking, a straightforward solution is provided: creating digital records validating each ballot's legitimacy while eliminating any possibility of tampering or recording inconsistencies [20].

The main problem facing the traditional voting system is the transferring of the election boxes (containers) from the data centers to the IHEC offices, which consumes time and resources, rather than the security issues related to destroying, losing, or tampering votes. Using blockchain will eliminate those problems by providing real-time, secure, and transparent transfer of the votes of citizens accurately. The introduction of blockchain techniques erases these issues by allowing instant, real-time digital recording of every vote result—all managed through software programs that streamline data creation as well as access [21].

Transparency is a key factor in democratic exercises. Voter concerns towards the trustworthiness and impartiality of vote counting derive fundamentally from verification procedures where citizens demand traceable procedures which enable them to validate that

Table 1. Traditional and blockchain-based comparison.

Traditional Manual Vote Transfer	Transfer of Votes Using Blockchain
Citizens visit polling stations during specified hours and cast their votes on paper ballots in private booths.	Citizens visit polling stations during specified hours and cast their votes on paper ballots in private booths.
Physical paper ballots are collected and secured in sealed containers to preserve their integrity.	Physical paper ballots are collected and secured in sealed containers to preserve their integrity.
Election officials manually count and tabulate the votes, potentially leading to human errors or oversights.	Blockchain technology ensures the accuracy and integrity of votes by creating an unalterable record of each vote.
Logistics involved in transporting physical ballots from various polling stations to a central counting location can be challenging and time-consuming.	Votes are digitally recorded on the blockchain in real-time, eliminating the need for physical transportation and reducing logistical challenges.
Limited transparency, as only a select number of individuals (e.g., election observers) are present during the manual vote-counting process.	Blockchain provides transparency by allowing all stakeholders, including election observers and the public, to access and verify the recorded votes in real-time.
Verification and auditing processes for manual votes may require significant time and effort.	Votes recorded on the blockchain can be easily verified, reducing the time and effort required for verification and auditing.
Manual vote transfer is vulnerable to potential human errors, fraud, or tampering.	Blockchain ensures the security and immutability of votes, minimizing the risk of human errors, fraud, and tampering.
Limited ability to track the movement and status of individual votes during the transfer process.	Blockchain enables real-time tracking and monitoring of each vote, providing an auditable trail and increasing transparency.
Overall, manual vote transfer relies heavily on human efforts and introduces potential vulnerabilities in terms of accuracy, security, and transparency.	Blockchain-based vote transfer enhances accuracy, security, and transparency, minimizing human errors and fostering trust in the electoral process.

their rights were exercised well using all due diligence. Blockchain-based procedures allow all stakeholders—public eyes like election observers—to access and scrutinize recorded public records' accuracy and honesty, guaranteeing a high-integrity outcome [22].

Within the blockchain, the verification mechanism differs from the traditional system. The traditional system is considered cumbersome since assessment requires a detailed and manual assessment. In blockchain, the auditing mechanisms available through blockchain methods easily provide digital signatures that encode singular authentication criteria. They also quickly track secure data flows, leaving no space for potential copycats-related attacks, which were limited in traditional systems and are now effectively addressed in digitized systems [23].

4.1. Blockchain-based voting implementations

Many countries and global organizations have employed blockchain technology to enhance both the security and transparency of electronic voting, with two main implementations including **Estonia's e-voting system** and **Voatz in the U.S.**

4.1.1. Estonia's e-voting system

In the field of digital governance, Estonia has become one of the world's leading countries. It introduced electronic voting (E-voting) by the end of 2005, relying on known cryptographic technologies rather than blockchain technology. Many researchers have discussed the effectiveness of this system and proposed incorporating blockchain technology

to further improve voting integrity and auditability. Managers have tested the election with Keyless Signature Infrastructure (KSI) blockchain, which enhances data security and ensures that election data remains tamper-proof [24].

The strengths of E-Voting are that it has a high voter turnout, a strong digital ID system, and continuous security improvements. While the challenges for it are not fully blockchain-based yet, reliance on government-controlled infrastructure.

4.1.2. Voatz (United States)

Voatz is a blockchain-based mobile voting platform used in pilot programs in West Virginia, Utah, and Colorado. The system employs blockchain for vote verification, ensuring end-to-end encryption and immutability. Voatz utilizes a permissioned blockchain (Hyperledger Fabric) rather than a fully decentralized one, allowing election authorities to maintain oversight [25].

The strengths of Voatz are that it improved accessibility, especially for overseas and military voters, and enhanced security compared to traditional online voting. The challenges for it are security vulnerabilities, concerns over privacy, and skepticism about blockchain's effectiveness in large-scale elections.

5. Proposed system

The proposed system incorporates revolutionary blockchain technology to ensure the utmost security of voting transactions, truly representing people's voices. This innovative solution is composed of four distinct phases that work seamlessly together: the voting process, blockchain network, consensus mechanism, and electoral server, as shown in Fig. 1.

5.1. Phase 1: Voting process

The voting process begins at the voting center, where citizens exercise their democratic rights by casting their votes using traditional paper ballots. They follow the familiar process of entering private booths, marking their choices, and placing the completed ballots in secure containers. This phase ensures that the votes are captured accurately and maintains the secrecy of each voter's choices.

This phase is a traditional phase, and the system does not affect it. The output of this phase is scanned, and the results are converted digitally. Usually, a flash disk is used to transfer the votes, which is an unsecured method. Now, the scanned votes are added to the blockchain, as in Phase 2.

5.2. Phase 2: Blockchain network

As soon as the voting process reaches individual votes and they are cast, the next phase begins with transferring the voting data from its location to the blockchain network. This network consists of numerous interconnected nodes, each of which represents an election center's computer. Those nodes operate as a swarm of nodes that work cooperatively in a decentralized, untrusted environment to ensure the security and transparency of voting data.

As soon as the voting process is done, each vote is registered electronically. Once converted into a secure digital format, its confidentiality and integrity are kept using the blockchain where it is recorded as a block content within the blockchain; at the end of the election process, it will be called tamper-proof election ledger. This is accomplished by scanning the ballot paper and then adding it to a shared pool of unconfirmed votes,

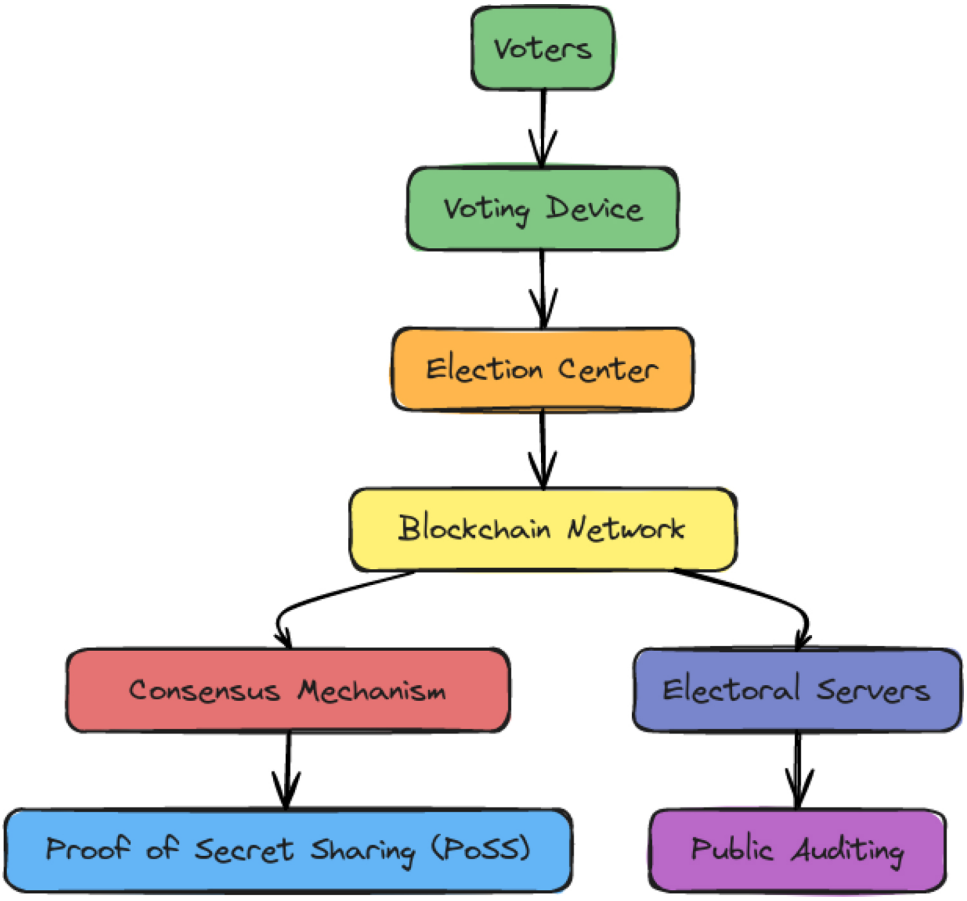

Fig. 1. Proposed system architecture.

known as the vote pool. This pool is used in the process of forming the block and it is appended to the blockchain.

For the purpose of blockchain immutability, each block added to the blockchain ledger has a special data structure form by connecting it to the previous node via a **hash code**; these codes have tamper proof purposes hashes for both current and previous block and this is why no block can be modified alone since the current block's data (votes and election-related metadata) and a timestamp marking the block's creation. Additionally, in this system, the information about the election center that contributed to the block are recorded within the block's body and the hash is calculated for the whole block.

The process of converting the paper election into digital form is done using **automatic counting devices.** The decentralized architecture ensures that each election center contributes to the global vote count and forms the block's primary data. These data are secured for every voting using cryptographic hashing, decentralized nodes, and time stamping which provide a transparent and tamper-proof record.

5.3. Phase 3: Consensus mechanism

For the verification and authentication of the data within the blockchain, the system employed a consensus algorithm which ensures the accuracy and integrity of voting, preventing fraudulent or unauthorized entries. This system employs a special consensus

algorithm named **Proof of Secret Sharing (PoSS)**, which is designed to safeguard the election process through a robust validation framework.

This consensus algorithm (PoSS) starts by distributing a share of the secret to every single node, which in our case is the election center, and this is done at a time prior to the election date. The authority responsible for selecting the secret and then generating the shares using secret sharing is the IHEC, and these shares are valid only during the predefined voting period.

These shares serve a dual purpose: they identify the election center and enable the secure addition of new vote blocks to the blockchain.

The PoSS process works as follows:

1. Each election center (node within the blockchain) submits its final votes and adds them to the blockchain, and initiates the consensus request by sending its secret share to the IHEC.
2. Any other nodes that were online at the same time within the network will validate this request by sharing their own shares for node verification.
3. The system is set by the minimum number of nodes needed for consensus, and once this number is available, the secret is collaboratively regenerated using their nodes and the requester node and this is its authentication.
4. After the authentication of adding a node is done, its data will be sent to the pool and it is ready to construct a node to add it to the blockchain.

This PoSS mechanism is not only used to verify the validity of the added nodes and the links of the chain, but it also ensures that only authorized election centers contribute to this process and that no one can add random data without authorization. By involving multiple nodes in the validation process, the system becomes resistant to tampering and fraud, reinforcing the security and trustworthiness of the electoral process.

5.4. Phase 4: Electoral server

After the addition of the verified votes by the verified nodes, this phase represents the transferring method of the distributed ledger to the electoral server**,** which serves as the central repositories for all votes. These servers, which generate shares after selecting the secret in the first place, act as authoritative source for saving, auditing, and counting the final votes. The distributed ledger, in which every single vote is written, ensures that every vote is recorded in a secure and immutable manner.

After the votes are securely stored on the servers:

- **Authorized authorities** can access the data for auditing or oversight purposes,
- **Media representatives** can review vote counts to provide timely updates to the public,
- **Voters themselves** can verify that their votes have been accurately recorded.

The blockchain network, through its decentralized nature and cryptographic safeguards, ensures the security and integrity of the votes during their transfer and storage. Each block in the blockchain represents a verifiable and unalterable record, providing an additional layer of transparency and trust.

To reach the highest level of security and privacy for the election process, many other technologies are combined with the blockchain, such as PoSS consensus and advanced cryptographic algorithms. This makes the final election system more resilient to known attacks on such a system, like tampering, unauthorized access, or manipulation, which, in turn, leads to building up confidence with voters and other stakeholders, as all votes are accurate, transparent, and verifiable.

The decentralized nature of the blockchain will provide some characteristics such as no entity whoever it represents within the system can control or manipulate the vote data. System's ability to provide immutable records offers the assurance of fairness and integrity in the electoral process. These additional levels of security enhanced the general security, privacy and transparency, making blockchain technology the only solution for every modern election system by ensuring that recorded votes are authentic and reflect the will of the voters.

6. Implementations

A sample of implementations is shown below:

```
New block was added to the blockchain.
Timestamp: 2023-06-22 13:45:00.123456
Votes: {'voter_id': 'Voter1', 'candidate': 'Candidate A'}
Hash: c4d8f9284f3e17e6b43c8f33e0e7a1d10f6c14eb2f02d7e26b6de7d5a9512345

New block added to the blockchain.
Timestamp: 2023-06-22 13:45:00.123789
Votes: {'voter_id': 'Voter2', 'candidate': 'Candidate B'}
Hash: 3a9e8b9c2d34567e98d1c0a4b5e6f7d8a9b4c3d2e1f0f5c9a8b7d6e5f4a3b2c1

New block added to the blockchain.
Timestamp: 2023-06-22 13:45:00.124567
Votes: {'voter_id': 'Voter3', 'candidate': 'Candidate A'}
Hash: 45b56c7d8e9f0a1b2c3d4e5f6a7b8c9d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5

Blockchain:
Timestamp: 2023-06-22 13:45:00.123456
Votes: {'voter_id': 'Voter1', 'candidate': 'Candidate A'}
Hash: c4d8f9284f3e17e6b43c8f33e0e7a1d10f6c14eb2f02d7e26b6de7d5a9512345
Previous Hash: 0

Timestamp: 2023-06-22 13:45:00.123789
Votes: {'voter_id': 'Voter2', 'candidate': 'Candidate B'}
Hash: 3a9e8b9c2d34567e98d1c0a4b5e6f7d8a9b4c3d2e1f0f5c9a8b7d6e5f4a3b2c1
Previous Hash:
c4d8f9284f3e17e6b43c8f33e0e7a1d10f6c14eb2f02d7e26b6de7d5a9512345

Timestamp: 2023-06-22 13:45:00.124567
Votes: {'voter_id': 'Voter3', 'candidate': 'Candidate A'}
Hash: 45b56c7d8e9f0a1b2c3d4e5f6a7b8c9d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5
Previous Hash:
3a9e8b9c2d34567e98d1c0a4b5e6f7d8a9b4c3d2e1f0f5c9a8b7d6e5f4a3b2c1
```

6.1. Block 1

Timestamp: 2023-06-22 13:45:00.123456
Votes: {'voter_id': 'Voter1', 'candidate': 'Candidate A'}
Hash: c4d8f9284f3e17e6b43c8f33e0e7a1d10f6c14eb2f02d7e26b6de7d5a9512345

To ensure data security, each block is assigned a hash value that reflects its content and is generated from the timestamp. The voting information in this block depends on the preceding hash being '0' as this block serves as the one, in the blockchain.

6.2. Block 2

Timestamp: 2023-06-22 13:45:00.123789
Votes: {'voter_id': 'Voter2', 'candidate': 'Candidate B'}
Hash: 3a9e8b9c2d34567e98d1c0a4b5e6f7d8a9b4c3d2e1f0f5c9a8b7d6e5f4a3b2c1

Similarly to previous blocks, this blocks' integrity is secured through a hash value that depends on its contents. The timestamp ensures that all timing aspects of each vote are captured accurately. The present block progresses after Block1 with a unique identifier created via generation from the prior hashed blocks.

6.3. Block 3

Timestamp: 2023-06-22 13:45:00.124567
Votes: {'voter_id': 'Voter3', 'candidate': 'Candidate A'}
Hash: 45b56c7d8e9f0a1b2c3d4e5f6a7b8c9d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5

The third vote, on the blockchain, was cast by 'Voter3' for 'Candidate A' like before. To ensure accuracy and transparency and protect data integrity over time, we use a method where each block is linked through hashing, making it nearly impossible to alter without the right decryption key. This process adds layers of security to every transaction recorded on the blockchain, ensuring transparency and irrevocability while building trust among all participants. Regular updates with timestamps and detailed transaction information are crucial in employing techniques to create unique "hash" values for each data piece. The consistent and logical connection between each linked element clearly shows that measures have been put in place to ensure the security of every transaction. Any effort to interfere with this system would lead to alterations that can be promptly recognized and rejected by all parties.

7. Results

The results section shows the improvements in blockchain behavior to handle high-volume data and scalability capability. Table 2 shows the obtained results, where TPS was increased by 37.84% with verification and finalization decreased by 84.14% and 87.39%, respectively, with a good reduction in CPU usage with the secure behavior of blockchain. These results show that the proposed system ensures secure delivery of votes data in a short period of time with small computational power required.

Table 2. Results.

Metric	Traditional System	Proposed System	Improvement (%)
TPS	100 TPS	137.84 TPS	↑ 37.84%
Verification Time (ms)	500 ms	79.3 ms	↓ 84.14%
Finalization Time (ms)	800 ms	101 ms	↓ 87.39%
CPU Usage (%)	40%	10.42%	↓ 73.94%
CPU User Time (%)	5%	0.0145%	↓ 99.71%

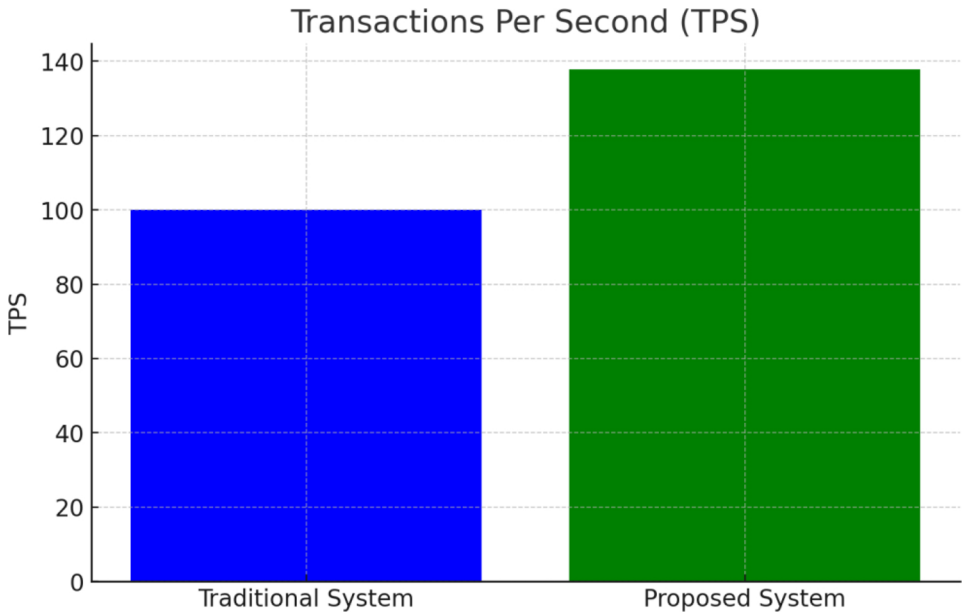

Fig. 2. Transactions per second (TPS).

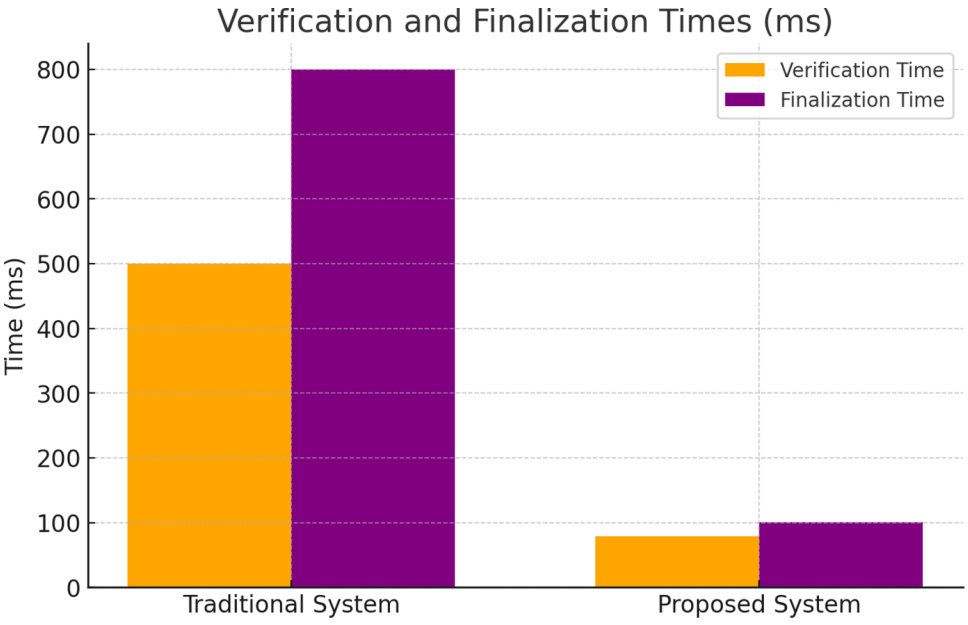

Fig. 3. Verification and finalization times.

Fig. 2 demonstrates the 37.84% improvement in TPS, showcasing the efficiency of the blockchain-based system in handling transactions compared to the traditional approach.

Fig. 3 shows the significant reduction in verification and finalization times for the proposed system. This highlights its ability to process votes quickly and efficiently, minimizing delays in the election process.

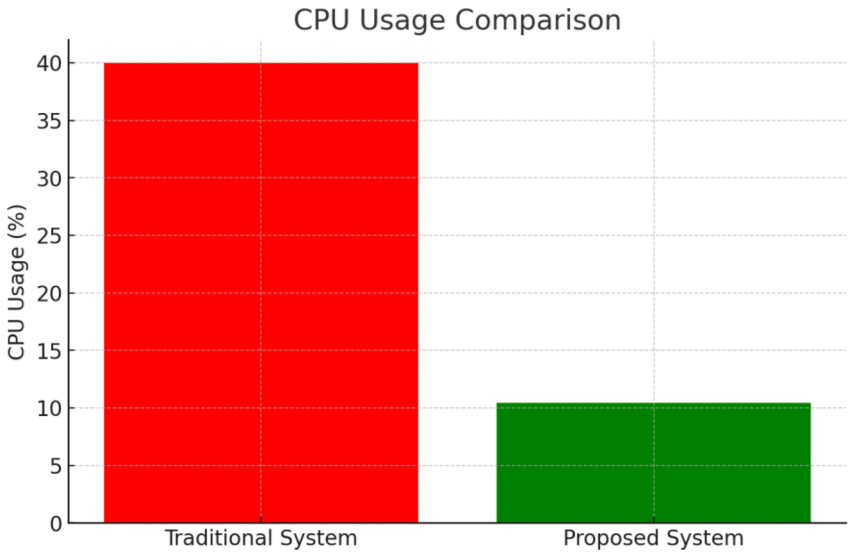

Fig. 4. CPU usage comparison.

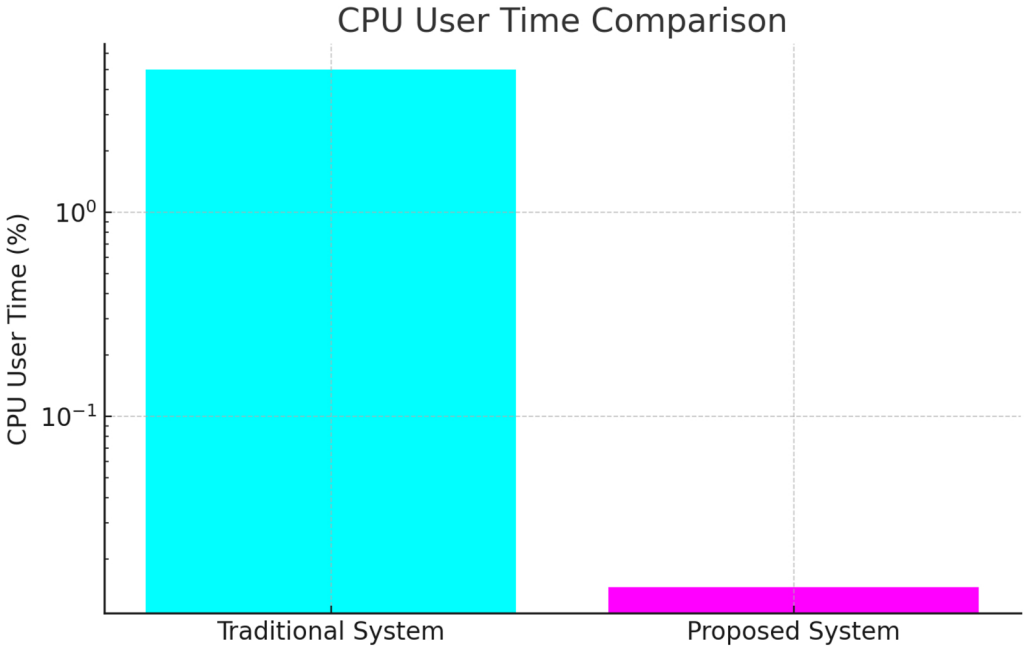

Fig. 5. CPU user time comparison.

Fig. 4 compares CPU usage for the traditional and proposed systems, emphasizing the lightweight nature of the proposed blockchain implementation.

Fig. 5 compares CPU user time comparison for the traditional and proposed systems, emphasizing the lightweight nature of the proposed blockchain implementation.

The PoSS method provides a unique approach to securing blockchain-based e-voting systems, differing significantly from traditional consensus mechanisms like Proof of

Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) in terms of authentication, decentralization, and resistance to attacks.

Unlike PoA, which relies on a small group of trusted validators, PoSS ensures that only verified election centers—pre-approved by the IHEC—can participate. This prevents centralized control and Sybil attacks, as election centers must present valid cryptographic secret shares to contribute votes. In contrast, PoA is vulnerable to authority compromise, meaning if the trusted validators are manipulated, the entire system's integrity is at risk.

Comparable to well-known consensus algorithms like PBFT, PoSS still requires multiple nodes for the validation of the votes, but it adds another layer of authentication which is done via secret sharing. To authenticate PBFT, two up to three honest nodes are still required for the presentation of the manipulation on data PoSS, and this is mitigated by enforcing multiple node secret construction, which makes unauthorized voting submission significantly more difficult.

Another key distinction is scalability. Other consensus algorithms, such as PoA, offer high efficiency within the scalability by using a small set of validator's nodes for the transactions. This is why PoA is considered ideal for private blockchain. PBFT, on the other hand, becomes less efficient as the network size increases due to its high communication overhead. PoSS strikes a balance, as it is agreed that more election center participation in the process improves security but, on the other hand, slows down the validation process and authentication of the adding node itself if too many nodes participate in the consensus.

Moreover, PoSS introduces time-sensitive authentication, since this authentication and the validation process is based on the shares of the secrets that expire after the official voting time, usually between 6 to 8 hours. This will prevent fraudulent votes from being submitted after elections conclude. This differs significantly from PoA and PBFT, both of which lack the ability for period constraints, making it suitable for continuous blockchain applications rather than election processes.

Ultimately, PoSS emerges as the most suitable consensus mechanism for blockchain-based e-voting, prioritizing security, decentralization, and attack resistance over speed. But PoA is still the best choice for an enterprise application where the power and trust are placed in a few known validators, especially in financial applications. By leveraging PoSS-based multi-node authentication and cryptographic secret sharing, blockchain e-voting systems can ensure election integrity, voter privacy, and verifiable transparency, making it a transformative solution for modern elections.

8. Discussion

The proposed blockchain-based system excels in multiple areas, it employs PoSS which provides some additional characteristics to the system such as high-speed transactions and guarantees security and tamper-proof mechanisms. The drastic reduction of the time required for verification and finalization times makes the system very useful for the large-scale elections and the less amount of required computation resources, such as CPU usage, shows that the system can work on limited computational resources which is an advantage if such system is adopted in regions where infrastructure is poor.

All the results are compared to previous studies, which aimed to accelerate validation times and achieve a 20% improvement in TPS, and did not optimize CPU usage, while the proposed system superior performance metrics demonstrate its efficiency and scalability, particularly in handling high voter turnout with minimal computational overhead.

PoSS consensus algorithm enhances security within the blockchain-based e-voting system by ensuring that only authorized parties (in this case, valid election centers) participate

in the blockchain contribution, with built-in mechanisms for mitigating major attack vectors such as Sybil attacks and 51% attacks.

In this election system, to prevent Sybil attacks, where an adversary creates multiple fake nodes (election centers) to manipulate the network, PoSS starts by assigning a unique share of the secret to each authenticated node for the verified election centers before the election process itself. Due to the collaborative nature of the system's nodes, these shares generate the secret again.. Attackers then need some kind of control over multiple election center more than or equal to the pre-defined threshold of nodes needed for reconstructing the secret which is highly improbable due to government-controlled distribution. Digital signatures and time-limited secret shares further strengthen this security layer.

And for 51% of attacks counter, since the PoSS enforces a multi-node authentication process which requires multiple independent centers to validate each vote and the natural restriction over times for using the shares, making long-term control infeasible in addition to further measures applied such as geographical distribution of nodes and votes verification using random centers. This will ensure that no single entity can dominate the voting process.

9. Conclusions

Adding technology into the election process raised the level of security, transparency, and integrity at all stages of the election. Employing a consensus algorithm proof of secret sharing adds a layer of validation to ensure votes' authenticity before they are added into the blockchain itself. Once confirmed, the votes are securely transmitted to the main servers and turn into an accessible, auditable, and verifiable record. This blockchain-based system guarantees the vote's security and integrity through decentralization, cryptographic methods, and consensus mechanisms, fostering trust in the process by offering a tamper-resistant platform for recording and tallying votes.

Acknowledgment

None.

Authors' contributions

Mohanad A. Mohammed conceived the system design and implementation, encryption model, performance evaluation, and manuscript preparation; Hala B. Abdul Wahab contributed to the manuscript; both authors reviewed and approved the final version of the manuscript.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this study.

Data availability statement

The dataset record was collected manually from the Iraqi IHEC site, and the data was formatted and split into different election centers. Available at: https://ihec.iq/the-results-of-the-parliament-elections-2021/, Election form sample: https://ihec.iq/28166-2/, Election data used: https://ihec.iq/29239-2/.

References

1. R. S. Al-tmimi and K. E. Grisham, "Elections as a tool for political participation in Iraq," *International Journal of Contemporary Iraqi Studies*, vol. 7, no. 3, pp. 233–249, Sep. 2013, doi: 10.1386/ijcis.7.3.233_1.
2. E. Daraghmi, Eman, A. Hamoudi and M. Abu Helou, "Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology in the context of Palestine," *Future Internet*, vol. 16, no. 11, Art. no. 388, Oct. 2024, doi: 10.3390/fi16110388.
3. M. A. Mohammed and H. B. Abdul Wahab, "Proposed new blockchain consensus algorithm," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 20, pp. 162–176, Oct. 2022, doi: 10.3991/ijim.v16i20.35549.
4. Y. M. Wahab *et al.*, "A framework for blockchain based e-voting system for Iraq," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 10, pp. 210–222, May 2022, doi: 10.3991/ijim.v16i10.30045.
5. M. H. Jumaa and A. C. Shakir, "Iraqi e-voting system based on smart contract using private blockchain technology," *Informatica*, vol. 46, no. 6, pp. 87–94, 2022, doi: 10.31449/inf.v46i6.4241.
6. H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, V. O. Nyangaresi and A. Y. Aldarwish, "Comprehensive challenges to e-government in Iraq," In *Proc. of 13thComputer Science On-Line Conf. 2024*, pp. 639–657, doi: 10.1007/978-3-031-70300-3_47.
7. S. Pandya, A. Raiyani and K. Vaghela, "A decentralized, secure, and transparent blockchain-enabled e-voting for Indian elections based on UIDAI Aadhar identification," In *Proc. of the Int. Conf. on Smart and Sustainable Developments in Engineering and Technology*, Vadodara, India, 21–22 May 2022, doi: 10.1063/5.0169194.
8. W. Salman, V. Yakovlev and S. Alani, "Analysis of the traditional voting system and transition to the online voting system in the republic of Iraq," in *Proc. of the 2021 3rd Int. Congr. on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, pp. 1–5, doi: 10.1109/HORA52670.2021.9461387.
9. Y. Abuidris, R. Kumar, T. Yang and J. Onginjo, "Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *EtrI Journal*, vol. 43, no. 2, pp. 357–370, Nov. 2020, doi: 10.4218/etrij.2019-0362.
10. Y. M. Tabra, "A proposal for internet voting system in Iraq," *International Journal of Advanced Research in Computer Science and Software* Engineering, vol. 3, no. 10, pp. 47–52, Oct. 2013.
11. S. B. Alkhakani and S. M. Hassan, "Suggest trust as mediation to adopt electronic voting system in Iraq," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 17, pp. 5729–5739, Sep. 2018.
12. Z. J. M. Ameen, "Application voting system of web-based in Iraq," *Iraqi Journal of* Science, vol. 58, no. 1A, pp. 192–200, 2017.
13. S. Tanwar, N. Gupta, P. Kumar and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1449–1480, May 2023, doi: 10.1007/s11042-023-15401-1.
14. P. Shelke, S. Dedgaonkar, N. Gopale, R. Desai, N. Deogaonkart and N. Joshi, "Blockchain-based e-voting system using smart contract," in *Proc. of the Joint Int. Conf. on AITC and CSSP*, Feb. 18, 2023, pp. 55-60.
15. M. A. Mohammed and H. B. Abdul Wahab, "A novel approach for electronic medical records based on NFT-EMR," *International Journal of Online & Biomedical Engineering (iJOE)*, vol. 19, no. 5, pp. 93–104, April 2023, doi: 10.3991/ijoe.v19i05.37589.
16. T. A. Jaber, "Security risks of the metaverse world," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 13, pp. 4–14, July 2022, doi: 10.3991/ijim.v16i13.33187.
17. Rahul, P. Gulia and N. S. Gill, "Articulation of blockchain enabled e-voting systems: a systematic literature review," *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, Art. no. 142, April 2025, doi: 10.1007/s12083-025-01956-3.
18. M. H. Berenjestanaki, H. R. Barzegar, N. El Ioini and C. Pahl, "Blockchain-based e-voting systems: a technology review," *Electronics*, vol. 13, no. 1, Art. no. 17, Dec. 2023, doi: 10.3390/electronics13010017.
19. T. A. Jaber, "Artificial intelligence in computer networks," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 1, 309–322, Jan 2022, doi: 10.21533/pen.v10i1.2616.

20. U. Jafar, M. J. Ab Aziz and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, Art. no. 5874, Aug. 2021, doi: 10.3390/s21175874.
21. M.-V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023, doi: 10.1109/ACCESS.2023.3253682.
22. C. D. González, D. F. Mena, A. M. Muñoz, O. Rojas and G. Sosa-Gómez, "Electronic voting system using an enterprise blockchain," *Applied Sciences*, vol. 12, no. 2, Art. no. 531, Jan 2022, doi: 10.3390/app12020531.
23. T. A. Jaber, "Sensor based human action recognition and known public datasets a comprehensive survey," in *Proc. Al-Kadhum 2nd Int. Conf. on Modern Applications of Information and Communication Technology (MAICT)*, Baghdad, Iraq, 8–9 Dec. 2021, doi: 10.1063/5.0119274.
24. G. Schryen and E. Rich, "Security in large-scale internet elections: A retrospective analysis of elections in Estonia, the Netherlands, and Switzerland," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 729–744, Dec. 2009, doi: 10.1109/TIFS.2009.2033230.
25. S. Kothari, S. Koparde, S. Joshi and N. Joshi, "TrustChain: A blockchain-enabled verifiable digital voting solution for election integrity," *Ingenierie des Systemes d'Information*, vol. 30, no. 3, pp. 637–645, Mar. 2025, doi: 10.18280/isi.300308.