Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Security Attacks on E-Voting System Using Blockchain

Saba Abdulbaqi Salman [1,*], Sufyan Al-Janabi [2], Ali Makki Sagheer [2]

[1]Aliraqia University, Baghdad, Iraq
[2]University of Anbar, Ramadi, Iraq

*Corresponding Author: Saba Abdulbaqi Salman

DOI: https://doi.org/10.52866/ijcsm.2023.02.02.016
Received December 2022 ; Accepted March 2023 ; Available online May 2023

ABSTRACT: E-voting become popular in many countries. Implement voting electronically to ensure a secure, reliable voting and tallying process. Blockchain technology may use a robust, trustworthy public ledger for saving votes. Despite that, many cyber-attacks are possible to affect either the miner or the Blockchain. Accordingly, this paper proposed an e-voting system based on Blockchain that provides (privacy, anonymity, and authentication). Cyber-attacks have been simulated using NS3 to test the backbone of the proposed approach. The results show increasing the number of sites and blocks in each Blockchain may eliminate most of the cyber-attacks like the 51% attack and Sybil attack. Tests on the authentication system show perfect face and QR code recognition system. Lastly, using the homomorphic achieves privacy and anonymity by tallying ballots without revealing the voter's personality.

Keywords: E-Voting, Cryptography, Blockchain, Security Attack

1. INTRODUCTION

Elections are one of ways for achieving democracy in societies nowadays. The beginning of democracy belongs to 507 BC in old Athens. And that was simple for face-to-face democracy. The next era of democracy was choosing representatives after the rise of national states in 1846 in Europe. After the Internet's invitation began the automation revolution in many areas like e-commerce and e-government. Because of the lack of information about the citizen's political directions, the need for e-democracy increased. Therefore, the first experience for e-election was conducted in Estonia in the 2007 elections [1]. The orientation towards e-elections spreads mainly in developed countries like the US, Australia, and Brazil. In contrast, this direction is still weak in many countries in Africa and Asia because of technical and cultural reasons [2]. In spite of the possible fraud cases, distortion of data, or falsification, the voting process is the primary democratic way for people to express their ideas and choices. Voting via paper is affected mainly by manipulation, damage, forgery, and other accidents. Some countries led by the USA converted towards e-voting since there are many mediators between the data and the hazards associated with the ballot [3]. Because of fraud possibilities in paper-based elections, many countries have adopted electronic polls. Elections play a significant role in electing suitable persons for the specific task. The electronic voting document contains encrypted voting data that may be tampered with. As a result, this paper has suggested an electronic voting system based on blockchain public ledger.
. An election on Blockchain is a new direction to run the elections electronically and maintain its database to an immutable ledger so that no one can claim that vote is fraud [4] despite cryptography, that can protect the contact between clients and servers. Another type of threat can affect the servers or server-side credentials like the Blockchain ledger. The threats are cyberattacks like the denial-of-service (DDOS) attack that brought down many of the leading web servers in February 2000 [5]. The Sybil attack occurs when a fake identity can communicate with legitimate entities as a real one. Sybil affects the mining process, proof, or work, causing the 51% attack. Once the attacker controls most of the Blockchain, it will lose its trust [6]. There is also the selfish mining attack. The selfish attack targets the real miner to mine a fake or empty block that should not include in the real Blockchain. This would result in wasting the power of the miners [7]. Accordingly, many cyberattacks may threaten the Blockchain as a public ledger.

The problem that motivates this research is the need for an e-voting system based on Blockchain that can be immune against various cyberattacks.

Blockchain technology is essentially a public ledger of transactions or events recorded and stored in chronologically- and linearly-connected blocks. Later blocks then maintain the hash of previous blocks [8].
Blockchain is a decentralized system, which could be this technology's most distinguishing feature. Specifically, collaborating with the third-party organization or the central administrator is not essential, which is a very simple response to this topic. Another reason is the immutability and resilience of Blockchain technology is the second advantage of using this distributed ledger. The information included within the blocks of the Blockchain cannot be altered or removed since it is essentially impossible to do so. When an intruder possesses the incredible processing power necessary to overwrite or erase the information on all computers included in the Blockchain before the next block is recorded here, it is conceivable for that information to be altered or removed from the Blockchain. If the Blockchain comprises many computers, then the system becomes more secure and transparent because it employs the cryptographical hash chain. So that, tampering would be hard for the attacker because of resources consuming [9]. Blockchain technology increase reliability , robustness of the voting process because it's a secure, immutable vote store repository, thereby reducing the threat of vote tampering. Countries including Germany, Russia, Estonia, and Switzerland have begin to use this technology into their electronic voting systems. [10]. The Blockchain allows a fully transparent election while keeping all the voters anonymous [11]. Therefore, the contribution of this paper will be, first, to provide an architecture design of an e-voting Blockchain system that provides anonymity, privacy, and authentication. Second, test the proposed e-voting system against various cyber-security attacks that may affect the miner or Blockchain. The next sections of this papers are : related word , blaockchain , procand cons of e-voting systems that based on Blockchain , Blockchain attacks, proposed system , experimental Results , lastly, the conclusion.

2. Related works

This section takes two related works; the first is related to the cybersecurity attacks on the e-voting system based on Blockchain. These papers discussed the attacks that targeted the Blockchain structure generally. The second is the papers that tackled various Blockchain e-voting proposed models and, if successful, to handle security, authentication, and anonymity issues.

Hanifatunnisa et al. (2017) created a traditional Blockchain e-voting system. The proposed system began creating a block, mining for a hash, and encrypting the hash using a public key for each node. The system achieves security by verifying the current block's hash The system was tested by a trail to create fake nodes. The verification system performed by all receiving nodes can identify if there are previous hashes and public keys that are not registered in the database. The counter-time system becomes a parameter when there are nodes with interference functioning per the design. The brut force attacking needs more time as the number of blocks increases. This paper did not handle the other types of cyber-attacks [12]. Khan et al. (2019) simulate a transaction malleability attack on a Blockchain e-voting system. The research found that transaction malleability may lead to block creation and mining delays. Transaction malleability is conducted by announcing two blocks, one fake and the second real. So, there is a chance to mine the fake block instead of the real one. The attack's success is measured by the number of miners that receive the mutated transaction first and the original transaction later. To succeed, the fake transaction must be broadcasted to the Blockchain network much faster than the actual transaction. The tests revealed that this type of attack may cause inconsistent Blockchain. The suggested solution against this attack is to speed up the mining for the honest blocks [13].

In 2019, Abuidris et al. proposed a hybrid Blockchain consensus protocol. They test their model against attacks simulated by Matlab. The hybrids consensus protocols comprised Proof of Credibility and Proof of Stake. The e-voting Blockchain system consists of three layers: one as a data center, the second for Blockchain serving, and the last layer for mining the new block.
The hybrid consensus with sharding security shows better efficiency in terms of security and latency time. Sharding, though, depends on dividing the Blockchain into sub-blocks, each with its private key can be encrypted. The paper doesn't talk in detail about the types of attacks, which is a fundamental limitation of this paper [15].

Cheema et al.(2020) have built a machine-learning model to detect DOS attacks on the backbone and Blockchain data center. The machine learning model predicts attacks and has been trained based on network traffic. The researchers used the USNWNB15 data collection to train the machine learning model. The data set has many regular traffic records with a traffic attack. Linear SVM was the best model, with 0.95 accuracy. The paper manages the case of a DOS attack [14]. Tas et al. (2020) deliver a literature review by studying the Blockchain-based e-voting system according to privacy into symmetric and asymmetric encryption. Tas has investigated 63 papers and analyzed them according to general, integrity, coin-based, privacy, and consensus factors. The study notes that privacy and transaction speed are most frequently emphasized issues facing Blockchain applications. The research handled the attack of DDOS and concluded that the system based on Blockchain could operate despite that attack because of the system's distributed nature [16]. Tas et al. in 2021 proposed a model in which administrators or miners are prevented from previewing election results, which are generally accessible data due to the Blockchain structure. A double-layer encryption model is proposed and tested in order to avoid manipulations that may occur with the election results. The system used homomorphic encryption to let third parties count the results without revealing the data to them. The voter needs a fingerprint to enter the system and cast the ballot. Although the system uses a permission-based private network, there may be Man-in-the-Middle, replay, or Sybil attacks. In case of incidents related to imitation of voters or attempts to change the vote cast, the results may be verified by cross-counting the votes in the election offices. But in real elections, the number of voters could be significant, making these types of attacks consume time [17].

The second part of the related papers is about the proposed e-voting system's architectures. We discussing here how the previous designers achieved privacy, authentication, and anonymity for Blockchain based e-voting system.

In 2018**,** Friorik et al. suggested a blockchain e-voting model that uses voter credentials, like username and ID card, to verify the voter from government identification service and establish a smart contract with a voter to verify the vote. The model uses a district node in traditional smart contract e-voting systems. The proposed approach is based on the implementation of a private blockchain. In this paper, each election process is represented by a set of smart contracts deployed on the Blockchain by the election administrators. A smart contract is defined for each of the voting districts [18]. In 2019**,** Tso et al. introduced the first Blockchain based noncentralized electronic voting and bidding systems. To improve privacy protection, they employed cryptographic techniques, such as indifferent transfer and homomorphic encryptions. This research combined SC and privacy-protection cryptography to create a distributed electronic voting system that allows voters to participate in the billing phase while also improving election efficiency. Because blockchain information is completely transparent and public, voter ballot information must be kept completely confidential before the billing phase begins. The proposed model allows voters and bidders to participate in the initiated process while keeping the voter anonymous, hiding data transmission privacy and data reliability and verifiability. Furthermore, compared to other electronic voting and bidding systems, the proposed models are safer and more efficient [19]. Yi et al. (2019) proposed techniques for leveraging the Blockchain in a peer-to-peer network to enhance e-voting security. The work enhanced the custom-programmed blockchain systems in three ways. First, the authors designed a synchronized voting record model based on distributed ledger technology (DLT). Second, they utilized a user credential model for authentication and non-repudiation based on elliptic curve cryptography (ECC). Finally, they employed a withdrawal model that allows voters to alter their vote before a specified date. A blockchain-based e-voting scheme for multiple candidates in a P2P network was proposed on Linux platforms for the essential requirements of the e-voting process by integrating the above designs. Electronic voting theory, cryptography, and software engineering theory were all used in the system. The testing results demonstrated a practical and secure e-voting system that solves the problem of vote forgery during e-voting. The Blockchain-based e-voting system can be directly used in various networking applications [20].
In 2022**,** Nasir et al. examined current blockchain solutions and proposed a new approach to achieving privacy and anonymity by combining two blockchains. Specifically, key management takes place on the first Blockchain, while anonymous voting is stored on the second Blockchain. The encrypted vote was hashed, salted with a nonce, and digitally signed with the voter's private key. The sequence in which the votes are cast was shuffled, and the timestamps of the votes were mixed to lessen the likelihood that the encrypted vote can be traced back to the voter. Using blockchain technology to implement this approach can significantly transform the current voting process by ensuring anonymity and privacy [21].

The previous papers discussed cyber-security attacks like DDOS, Tas [12], while others discussed man in the middle. In contrast, this paper takes a set of significant attacks in Blockchain. The attacks considered in this study targeted both miners, like the eclipse attack, and the Blockchain itself, like a 51% attack.

We rely on three principles (privacy, anonymity, and authentication) to compare our proposed model with previous models. Paper's Firorik achieved anonymity and authentication without privacy, the Blockchain environment's fundamental weakness.

Tso enhanced availability privacy without thinking about authentication. In contrast, Yi focused on privacy by encryption without anonymity, which is crucial to hide voter's information. Last, Nasir et al. did not tackle authentication and worked on privacy and cryptography. The proposed system achieved anonymity to keep voters' information hidden. Privacy to encrypt Blockchain data. Authentication to ensure that only real registered voters can enter the voting page.

3. Blockchain Technology

A new kind of distributed database called a Blockchain stores data in the form of immutable block structures. A Blockchain (chain of blocks) is created when all these blocks are connected to one another in a chain form, serving as a ledger. Every party in the network has a copy of the ledger to confirm each transaction or network operation. Each block has a predetermined size and contains the current block's hash value as well as the timestamp, the raw data, the source, the destination [22]. A complete order of blocks is essential for Blockchain because of this, every block has a pointer that directs users to the block that came before it in the chain of valid blocks. The point is specifically a hash of the block before it. Therefore, the Blockchain has the structure of the linked list, as shown in Figure 1 [23].

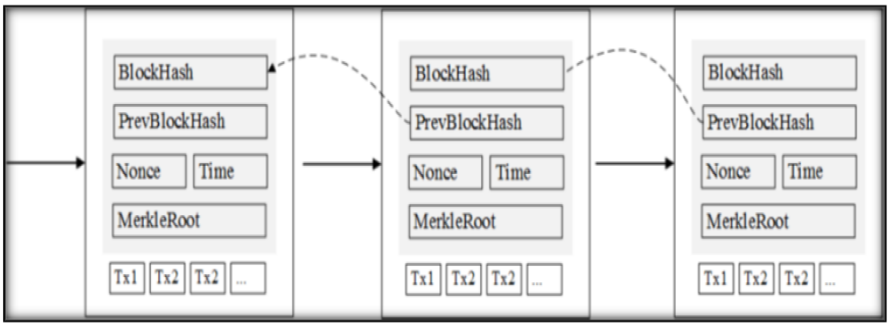

FIGURE 1. Blockchain Structure

4. Pros and cons of e-voting systems based on Blockchain

The conversion from the centralized e-voting systems to the blockchain-based e-voting has to be discussed carefully to specify the advantages that may lead to this conversion. At the same time, the drawbacks must be examined to address the weaknesses and vulnerabilities that may lead to big bugs in such a system. An open, decentralized, widely distributed, cryptographic, and immutable ledger potentially provides desirable properties to any voting system. First, Transparency is significantly increased in counting ballots stored on the Blockchain, as everyone can tally their votes . Second, with enough nodes, vast numbers of vote ledgers independently verify data, making it very difficult for hackers to try to cast fraudulent ballots. Third, using cryptography with blocks ensures data privacy and the authenticity of the votes from eligible voters. Last,

Blockchain voting could return a substantial amount of control over elections to the general population by empowering them and lessening the necessary authority of government —the summary of issues that may appear from adopting Blockchain for e-voting. Even if the system designer provides security through encryption for a blockchain system, there are vulnerabilities like voter-verifiability and contestability. Also, applying cryptography or any security techniques on distributed ledgers needs to be used over the system's sites. Although blockchain e-voting systems are immutable, it is still possible to be compromised by attacks like 51% for smaller blockchains. The last drawback is that if the voter lost his keys, the blockchain voting system must have a robust key management policy[24].

The proposed system in this research has considered all the possible potential drawbacks of taking the maximum benefits from using the Blockchain as a public ledger.

5. Blockchain Attacks

Blockchain attacks are attempts either to attack the network of the Blockchain or attack the mining process. In fact, there have been instances where blockchain-based e-voting systems have been targeted by attackers. For example, in 2020, Russia's blockchain-based e-voting system suffered a node attack [10]. Figure 2 depicts the numerous Blockchain threats, which include phishing, DDoS, selfish mining, eclipse, and 51 percent (51%) [7].

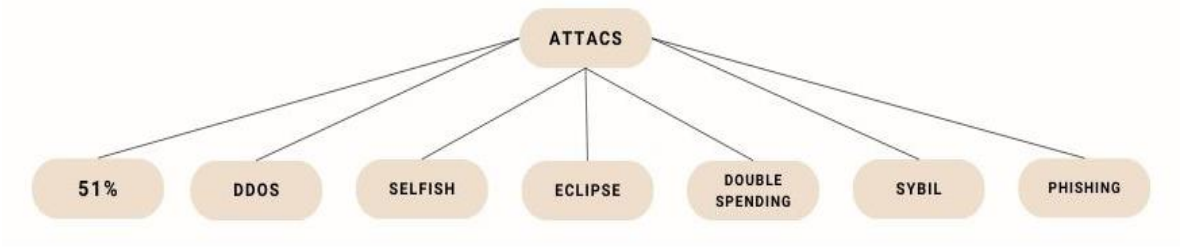

FIGURE 2. Attacks on the E-Voting System

5.1 The 51% attack

Another name for this technique is majority attack. The assault is carried out by miners, who control 50% of the computer power compared to other nodes. The attacker may be able to control the Blockchain by altering the transaction and validation processes, as well as the mining power, if this assault is conducted at a 51% level in the Blockchain. This offensive tactic or plan may shift or vary depending on the chosen consensus. In contrast to other consensus processes, the PoW consensus mechanism performs this function the majority of the time. Most often, cryptocurrencies like Bitcoin are subject to this assault. Attackers may manipulate the pace at which hashes are mined in this attack utilizing Blockchain technology based on cryptocurrencies, which would prevent confirmation of new transactions[8]. In the e-voting Blockchain system, a 51% attack can cause anomalies in the public Blockchain system, leading to double-spending or even overriding the transaction block [25].

5.2 The DDos attack

It is a kind of cyber-attack that overloads a network or a single node with more requests than it can handle, clogging up the network's traffic. As a result, users on the network won't be able to access network resources effectively, and the target node will also experience temporary downtime from being overloaded. This attack can only target a network node or the whole network. When an attacker targets a particular node, it repeatedly sends many requests to that node. As a consequence, the victim node is overloaded and unable to respond to genuine network requests. If this assault is conducted using Blockchain technology, the whole network malfunctions and sometimes becomes unusable for transactions. This exploit was just found on GitHub. This assault on blockchain technology targets cryptocurrencies like Bitcoin that utilize the technology. This attack targets the Bitcoin mempool, also known as memory pools (a repository for all transactions that have not yet been verified by the network) [9]. In the context of e-voting Blockchain, a DoS attack can be launched to overwhelm the Blockchain network with traffic, making it difficult or impossible for legitimate users to access the network [24].

5.3 The Selfish mining attacks

This assault is a malicious attack of some kind. Eyal and Sirer are credited as being the first to notice this attack (Saad et al., date). If this assault takes place on a Blockchain, it will jeopardize the integrity of the whole network. In this attack, a self-centered miner node will prevent a properly confirmed mined block from being sent to the rest of the network. They later begin mining the subsequent block to build their own private chain. Then, since this secret chain seems to be longer than the specific public Blockchain, all miners will attempt to add their blocks to it, believing it to be a real chain, wasting their computing power and resources. Thus, by engaging in this kind of mining, the self-centered miners will reap more benefits. The miners or mining pools that use a large network hash may launch this assault. Because additional joining nodes will be added to the selfish miner's chain if it becomes too lengthy, the selfish miners may also prevent other mining blocks from receiving rewards. These factors increase their benefits. This assault is also known as a "block withholding attack" since the self-centered miner prevents the block from being broadcast[5].

5.4 The Eclipse attacks

These attacks include a collection of malicious nodes controlling the incoming and outgoing traffic of its neighboring nodes and disconnecting them using their IP addresses. All nodes in the Blockchain network are interconnected. Each node is aware of the IP address of every other node. This attack will isolate the reliable node, manage its incoming and outgoing traffic, inject false data into it, and block that node [4]. In the Blockchain-based e-voting system, an eclipse attack is conducted when attacker controls all the nodes connected to a particular node, thereby refusing to relay any new blocks produced by miners [26]

5.5 The Double spending attacks

Attacks known as "double spending" involve the attacker spending the same money twice. This kind of assault is physically impossible. By submitting a transaction and then waiting until the merchant approves it and delivers the items, the attacker will start this process. Once again, the attacker will insert that amount into another transaction after blocking or reversing the communication with the merchant. To counter this exploit, recipient-oriented transactions were developed [27].

5.6 The Sybil attacks

John Douceur brought attention to this assault. In this assault, the enemy will create a sizable number of false nodes that mimic real ones in the network, which disturbs and confuses the whole network. These false nodes manipulate the network consensus, verify illegal transactions, or modify the transactional data. This assault becomes difficult to pinpoint if the attacker has control of a large number of nodes. Blockchain allows for the right use of consensus, which may prevent this assault. More often in peer-to-peer networks does this assault occur [11].

6. Proposed system

The proposed system is designed to achieve running election events, ensuring anonymity, privacy, integrity, and authentication. Gaining the mentioned goals required mechanisms in both the registration and voting process. The proposed system provides anonymity by encrypting the voter data with a regional public key belonging to the regional election office, at the same time, encrypting the vote by a homomorphic public key of the higher election commission. The reason for using homomorphic to encrypt the voice is to enable the higher commission to tally ballots without decrypting the votes. The encryption itself ensures privacy. Authentication is achieved by letting the voter enter the voting page by using his face biometric features and the voter's QR code.

A proposed system for electronic voting for the Iraqi elections was chosen. The proposed model is based on the following:

1. The Iraqi High Electoral Commission sends homomorphic keys to the front end of the voter, calculates the results, and announces them.
2. Sub-offices are defined as regional offices that verify the voter's authenticity and create a wallet for each voter. Send keys and certificates directly to the front end of the user and save the vote in block form in the database.
3. The system saves the block to the Blockchain database in the cloud. The could services provided by pyhtonanywhere free host. The database is SQLite installed inside the cloud host.

So, our e-voting system consists of two parts: registration and voting. The registration part is responsible for registering, save new voter information, and sending QR code key certificates via voter's mail after finishing registration. Key certification is a private RSA key to sign the block on voting day. The QR code (RSA private) is used to let the voter enter the voting page by scanning the QR code.

The voter must have their ID card to register in the voting system during the registration phase, and Iraq follows a similar procedure. The election committee initializes this card. Registration of a new voter is the first phase in the election process. The new voter must submit his/her information to the e-voting model with his/her picture to recognize him/her by the e-voting siftware and allow the voter to enter the election page. For large-scale elections (e.g., in national elections in Iraq), every voter must have a voting card to be an authorized voter. This card information can also be used in the registration step.

The registration phase begins when a new voter submits their information in the registration HTML form, including their first name, last name, gender, age, personal ID, and voter ID number. The voter must then upload a personal picture as part of the registration form. If successful, the registration form will be submitted for processing. After the submission process the voter's certificate, (QR code private key) will be send to the voter.

The biometric authorization will use the personal picture to let the voter enter the system. Figure 3 describes the new voter registration phase.

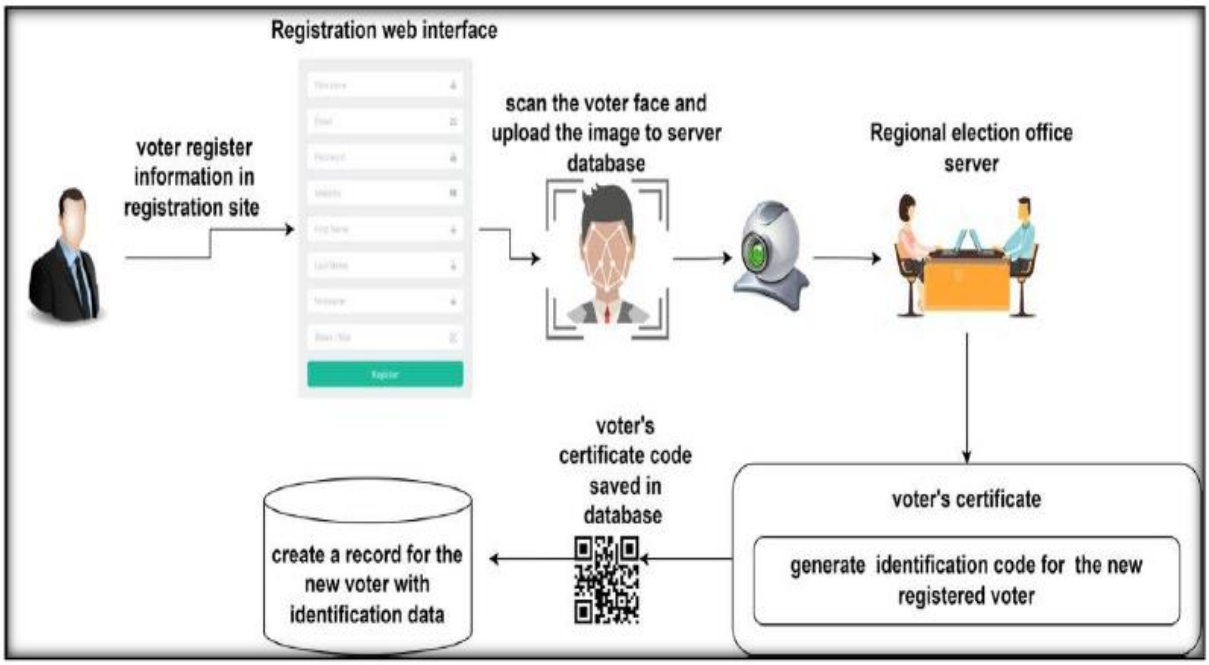

FIGURE 3. Registration Process

The election authority server saves the voter's submitted information and creates a wallet "record". The proposed registration part generates a private key using RSA cryptography for the newly registered voter. Then, the voter's private key is converted into a QR code picture that is sent later to the registered voter by his/her e-mail. The voter must keep his/her own voter's certificate (QR code private key) number in his/her device (e.g., cellular phone) to use it on election day. This QR RSA private key represents the voter's digital certificate that will be used later to sign personal data of the voter. The QR code web camera scanning is the second step to check the voter's personality after checking his/her face. The voter's certificate (QR code private key) code entrance saves the voter's privacy from being stolen or revealed. Scanning within the registration for the voter's face enables him to enter the voting chamber by his face. Then, for more authentication, the voter scans his private key's QR code as an additional tier of authenticity.

The second step is the voting step. In the election day voting process begins with voter's entering to the home page of the voting system, as shown in Figure 4.

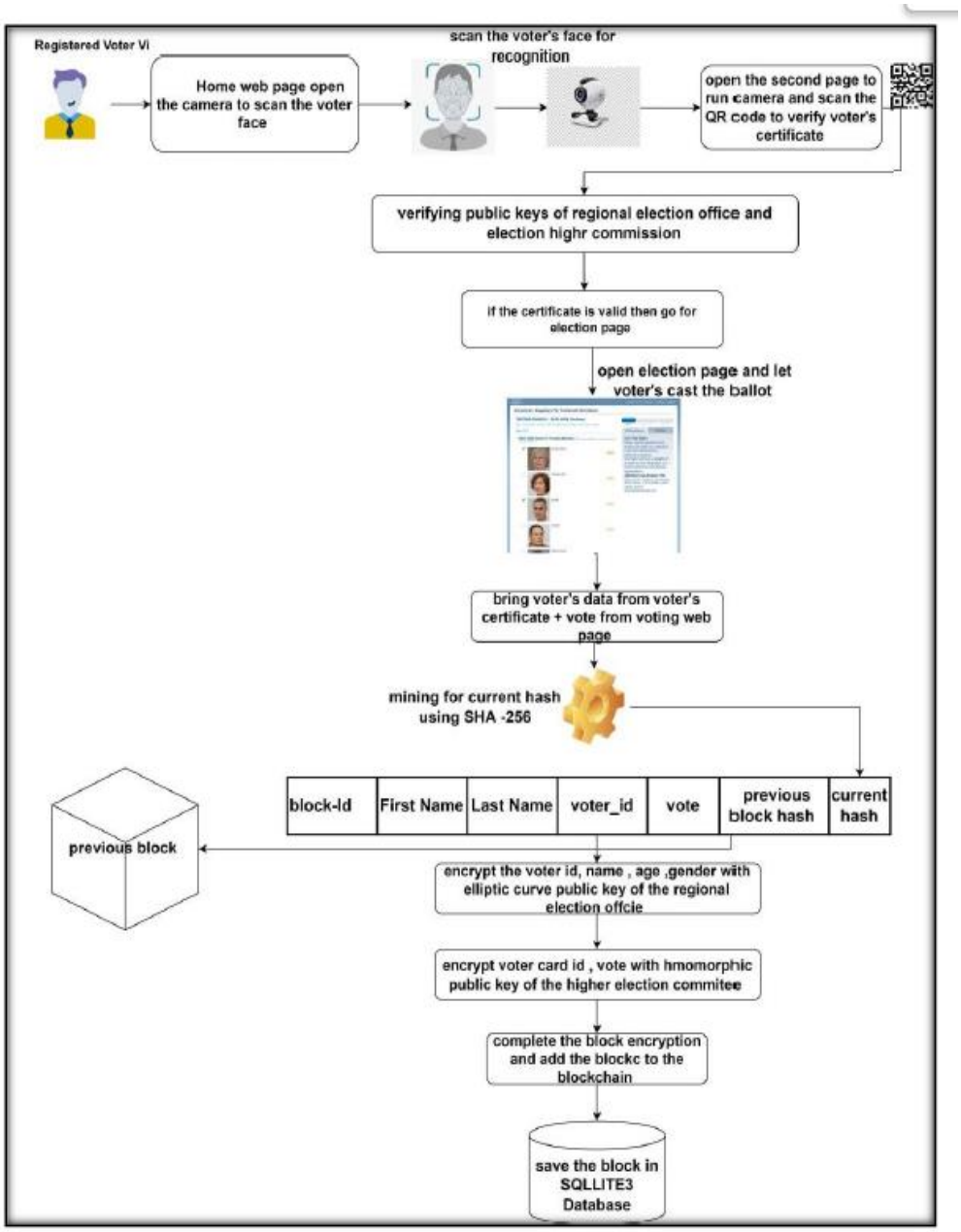

FIGURE 4. Entering the Home Page of the Voting System

The registered voter begins voting by entering the voting home page that operates the web camera in the voter's PC. Then, the voting model scans the voter's face as biometric authentication. If the face recognizer part recognizes the voter's face, the voter is redirected to the next authentication step.
The next page involves scanning the voter's certificate (QR code private key). The voter has the photo of his/her certificate (QR code private key) that must be redirected to the web camera; if the QR code recognition program recognizes the QR code in the voter's profile, the voter is then accepted to access the public key verifying page. Next, the public key validation process begins. This step comes when a voter is authenticated to vote. To this end, the voter may want to check the validity of the public keys for both the regional election office and higher election commission. Therefore, this validation is carried out by disseminating the public keys of the regional election office/ higher election commission using a digital certificate that contains the public keys and were signed with a trusted certificate authority's private key. In this regard, a digital certificate allows any voter to obtain the regional election office public key with higher election commission public key to obtain the digital certificate

and verify its validation through the attached authorized signature. The following steps clarify the process of checking the digital certificate for the regional election office:
1. The voter first asks the regional election office for the digital certificate.

2. The regional election office then prepares a digital certificate consisting of {election point ID number, election point public key, and higher election commission public key}, which are used to generate a hash.

3. The hash is encrypted with the certificate authority's private key.

4. The voter receives the unsigned part of the data with a certificate. The voter side then calculates the hash and decrypts the encrypted hash sent with the authority digital certificate public key to match and check the certificate validity.

The voter who received the certificate uses the authority public key *PUauth* to decrypt the certificate. Both ***IDA*** and ***PUa*** provide the recipient with the name and public key of the certificate holder. After the voter verifies the regional election office public key certificate, the voter is redirected to the voting page. The voting page contains a table of candidates who hold (candidate number, name, party number, and candidate picture). In particular, there is a text box to add the voter's card number. At the bottom of the page, the voter can choose the candidate and press the submit button. After voters choose a specific candidate and press submit, the flask server begins to execute the crucial part. Specifically, the flask server begins to initiate a lock for this vote to be linked with previous blocks that create a Blockchain. The flask application uses the voter card to get the information of the voter, including {first name and last name of the voter, age, address, and date}. Figure 5 below presents the mechanism of creating a block for each vote.

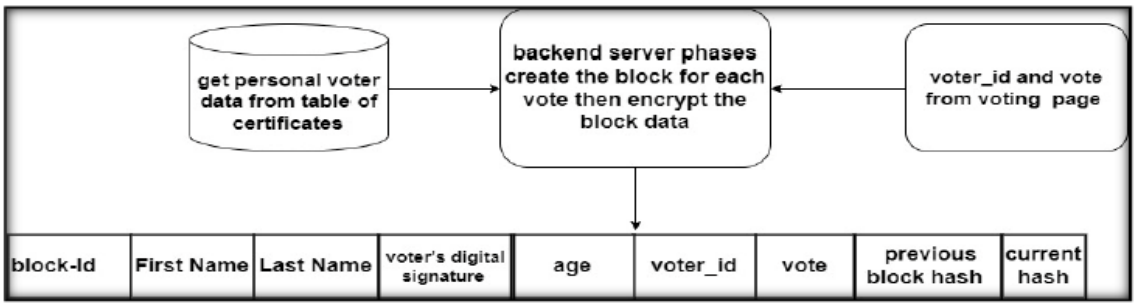

FIGURE 5. Mechanism of creating block

The next step is creating the new hash for the current block, where the model mines to find the new hash that accommodates the condition of hashes, which must begin with four zeros. After adding the new hash, the flask web system saves the block in the voting table inside the database using the database class function (insert).

The Blockchain is implemented in the proposed system as a class using Python language. This proposed system did not rely on existing platforms like Ethereum or Zcash. The blockchain part is written from scratch as an object-oriented class. When running the e-voting system by the Flask web server, each block is represented as an object in the server's memory and saved later inside the SQLite database. Figure 6 illustrates the process of creating a new block and adding it to the Blockchain.

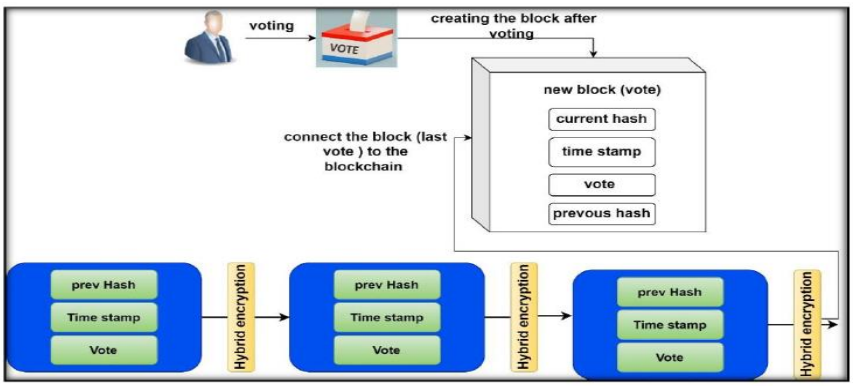

FIGURE 6. Adding a block to Blockchain

The block in figure 7 consists of the following data (ID, or the number of the block, f-name: the first name of the voter, l_name: the last name of the voter, address of the voter, phone number of the voter, voter_ID, which means the voting card number, and the vote or his/her choice in the election). Specifically, a single block is represented by 126 bytes in average. At the same time, the whole Blockchain can contain data without limit. The Blockchain depends on the size of the web host server that hosts the Flask website application.

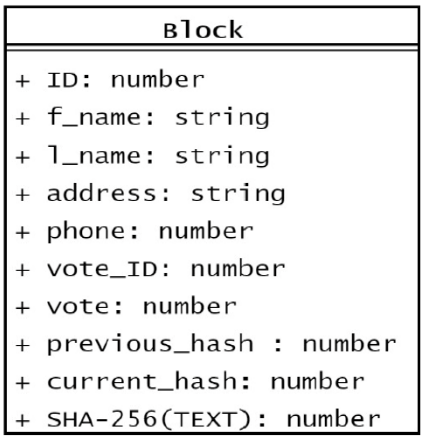

FIGURE 7. class representing a single block

7. Experiment and Results

This research's main experiments are about testing the immunity of the proposed e-voting system against cyber-attacks. The test is conducted by presenting 100 sites (Blockchains). Each site contains a miner. The minimum number of blocks in each Blockchain site is 100 blocks. The secondary experiments test the power of the encryption methods used in this proposed system. The test has been implemented using a Network simulator (NS3), an application that simulates algorithms for network scenarios. Ns3 began in 1989 as a variation of the REAL network simulator and was supported later by DARPA. The reason for choosing the NS3 is that it is cheaper and possible to test and evaluate models, mainly when the system may not be available because either complex or costly. We supposed that the proposed method consists of 100 sites. Figure 8 clarifying the general structure of the testing simulated system. Each one is regional and represented by a public ledger (Blockchain). In each area, the Blockchain saves the votes. Figure presents the general architecture of the proposed system tested using NS3

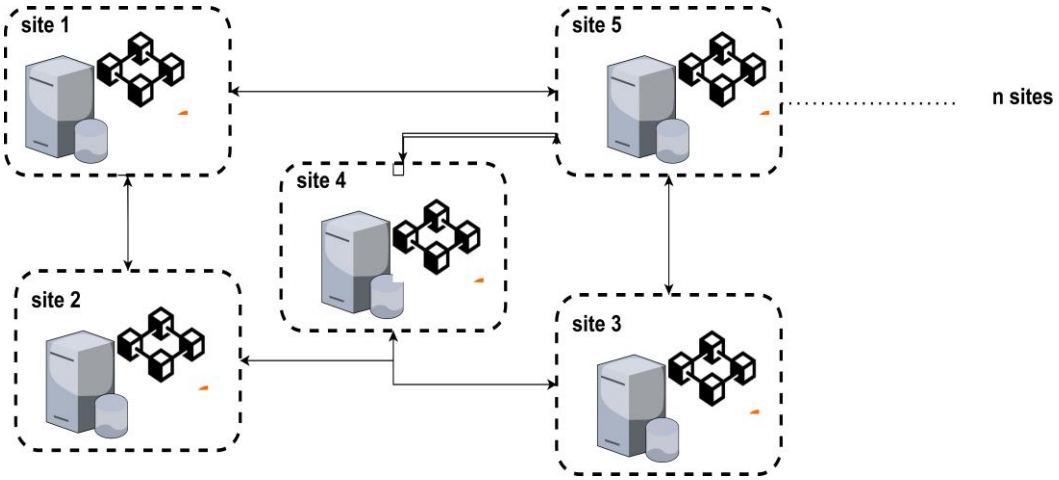

FIGURE 8. Proposed simulated blockchain e-voting system

The first is for an eclipse attack. This test was run to evaluate the time needed to attack miners in seconds according to the number of voting points (Blockchains); in the proposed design, there is a miner on each site. Figure 9 indicates that

when nodes increase, the attacker needs more time for an eclipse attack. The attacker needs 1600 hours to compromise 100 sites.

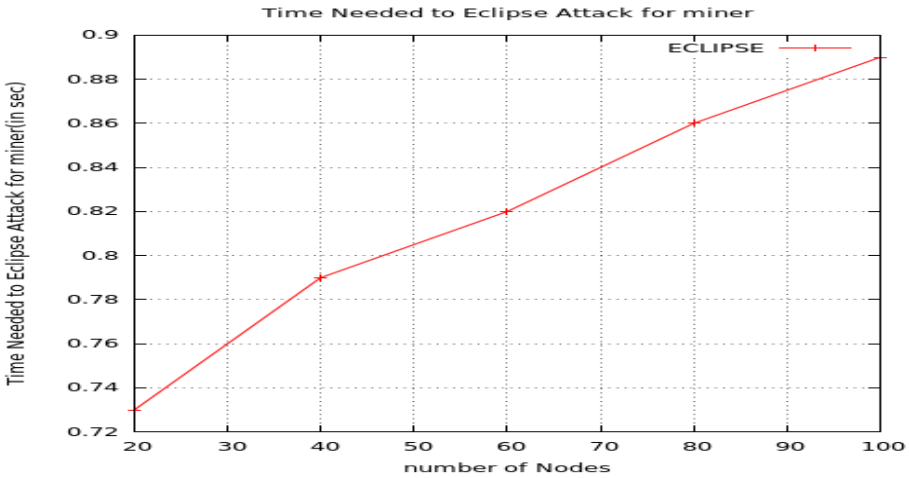

FIGURE 9. Eclipse attack measurements

Second attack tested was Sybil attack. This attack makes a fake miner participate in minning process instead of real miner. We simulated Sybil attack and the results is shown in figure 10 refers to the relation between the number pf blocks advertised for mining and the time consumed by Sybil attack.

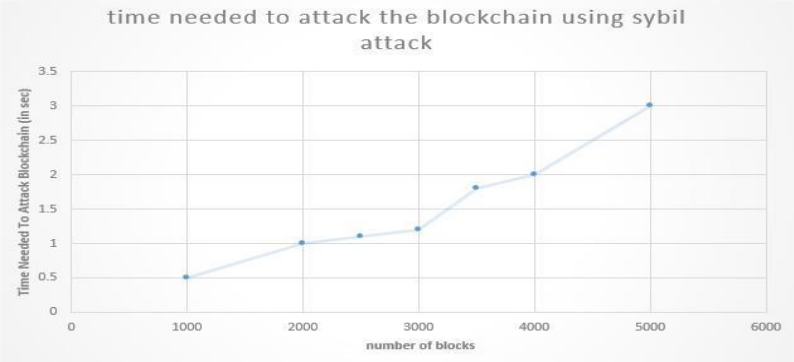

FIGURE 10. Time required for Sybil attack

If the Blockchain consists of three million blocks, the attacker needs about 30 minutes. As a result, we have to make the Blockchain large enough to reach security against Sybil. Or provide a mechanism to authenticate the miners.

The third attack is the DDos, simulated by overwhelming the miner with fabricated blocks. Figure 11 illustrates the results. The X-axis represents the number of blocks, while the y-axis represents the time. This attack needs more time according to the number of blocks.

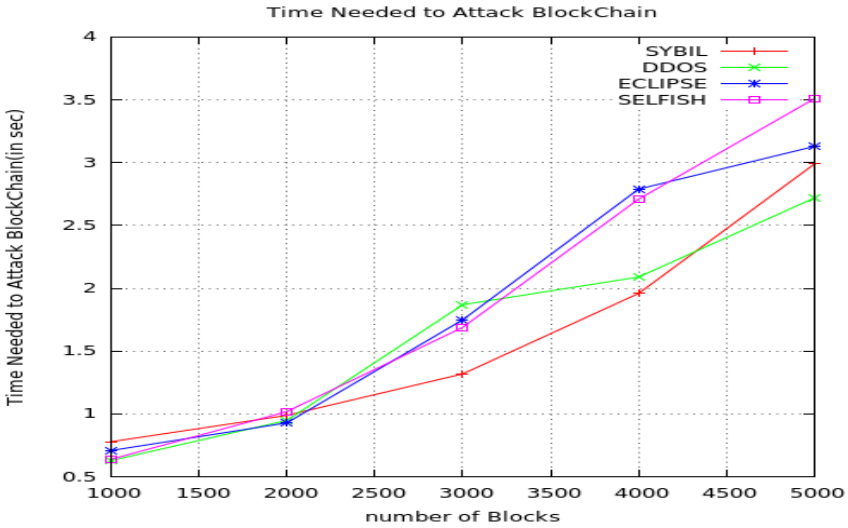

FIGURE 11. DDos time attacking

For instance, the number of blocks was 5000 blocks the attacker need 35 seconds. Therefore, this requires 11 hours to attack one million blocks, but if the system has 100 miners, the attacker needs 1.166 hours.

The second type of attacks the mining attack the test of 51% attacks need to build a provide chain that may replace the real Blockchain. Figure 12 refers to the may need to increase the number of blocks to 5million to secure the system against a 51% attack.

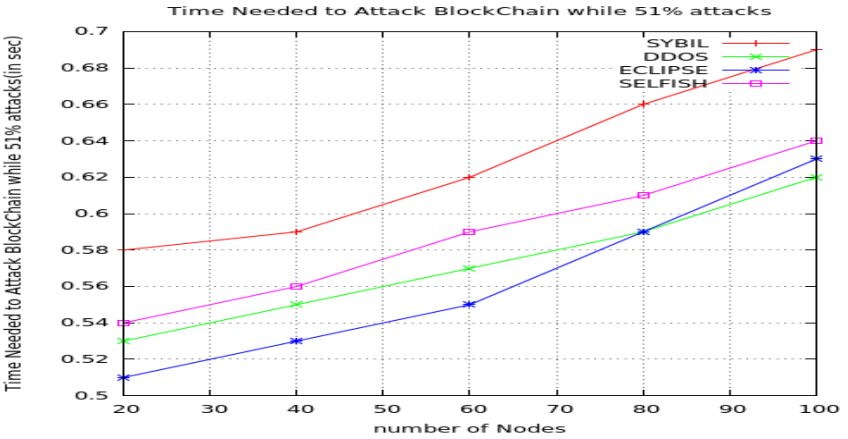

FIGURE 12. Time needed to attack 100 sites by 51% attack

The last attack is a selfish. This attack simulates the re-mining of the real block. In Figure 13, the x-axis is the number of nodes (sites). While the y-axis represents time needed to attack sites (blockchains). According to the test. If the attacker conducted an attack on 100 nodes, he will need about 0.56 seconds. This means that this attack is effective and dangerous to influence the authentication of the miners.

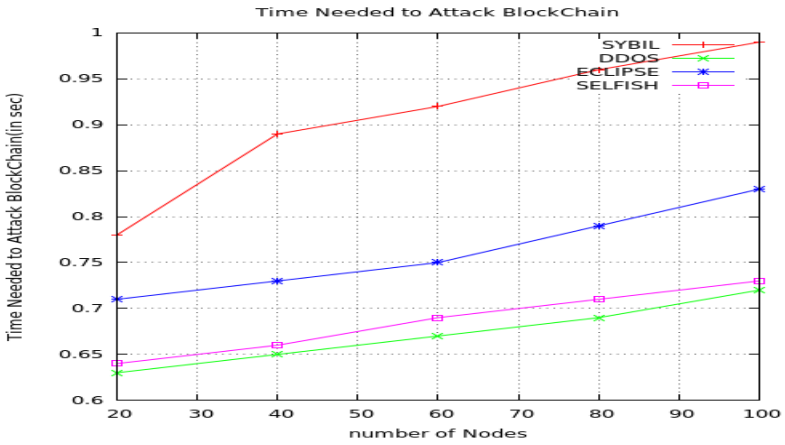

FIGURE 13. Time needed for selfish attack

By developing a low-cost, secure, transparent, and transparent voting procedure, Blockchain enables electronic voting applications.

8. Conclusion

Many countries recently converted to automate the voting process due to the reliability of the traditional paper-based election process. E-voting provides reliability, security, authentication, and anonymity. According to that, the problem of this work was how the e-voting system could be secured and repel the cyber-attacks on either blocks or miners (election sites). In this work, most possible Blockchain attacks were examined. So, the conclusion is that increasing the number of miners within the proof of work and consensus paradigm is crucial as a shield against cyber-attacks. Additionally, the proposed system provided privacy and anonymity through homomorphic encryption. Authentication by both face and QR code recognition to let legitimate voters participate in the election event.

Funding

None

ACKNOWLEDGEMENT

The first author would like to thank the reviewers for providing useful suggestions, allowing for the improved presentation of this paper.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] R. Krimmer, S. Triessnig, and M. Volkamer, "The Development of Remote E-Voting Around the World: A Review of Roads and Directions," in *E-Voting and Identity*, A. Alkassar and M. Volkamer, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 1–15.

[2] "Is e-voting currently used in any elections with EMB participation? | International IDEA." https://www.idea.int/data-tools/question-view/742 (accessed Sep. 04, 2023).

[3] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

[4] S. Latif and T. Anees, "Blockchain based Decentralized Electronic Voting System: A Step towards Transparent Elections," *IJCSNS*, vol. 19, no. 12, p. 165, 2019.

[5] A. D. Rubin, "Security considerations for remote electronic voting," *Communications of the ACM*, vol. 45, no. 12, pp. 39–44, 2002.

[6] M. Platt and P. McBurney, "Sybil attacks on identity-augmented Proof-of-Stake," *Computer Networks*, vol. 199, p. 108424, Nov. 2021, doi: 10.1016/j.comnet.2021.108424.

[7] M. Kędziora, P. Kozłowski, M. Szczepanik, and P. Jóźwiak, "Analysis of blockchain selfish mining attacks," presented at the International Conference on Information Systems Architecture and Technology, Springer, 2019, pp. 231–240.

[8] J. J. Xu, "Are blockchains immune to all malicious attacks?," *Financial Innovation*, vol. 2, no. 1, p. 25, Dec. 2016, doi: 10.1186/s40854-016-0046-5.
[9] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating Suitability of Applying Blockchain," in *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*, Nov. 2017, pp. 158–161. doi: 10.1109/ICECCS.2017.26.
[10] 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.
[11] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications*, May 2023, doi: 10.1007/s11042-023-15401-1.
[12] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, IEEE, 2017, pp. 1–6.
[13] K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain-based e-Voting," *Computers & Electrical Engineering*, vol. 83, p. 106583, May 2020, doi: 10.1016/j.compeleceng.2020.106583.
[14] M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, "Machine Learning with Blockchain for Secure E-voting System," in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, Nov. 2020, pp. 177–182. doi: 10.1109/SMART-TECH49988.2020.00050.
[15] 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, 2021, doi: 10.4218/etrij.2019-0362.
[16] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020.
[17] R. Taş and Ö. Ö. Tanrıöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," *Security and Communication Networks*, vol. 2021, p. 6673691, Apr. 2021, doi: 10.1155/2021/6673691.
[18] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, IEEE, 2018, pp. 983–986.
[19] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, "Distributed E-voting and E-bidding systems based on smart contract," *Electronics*, vol. 8, no. 4, p. 422, 2019.
[20] H. Yi, "Securing e-voting based on blockchain in P2P network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–9, 2019.
[21] V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, "Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain," *Applied Sciences*, vol. 12, no. 11, 2022, doi: 10.3390/app12115477.
[22] "Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions [Book]." https://www.oreilly.com/library/view/blockchain-a-practical/9781260115864/ (accessed Aug. 30, 2022).
[23] T. Jamsrandorj, "Decentralized Access Control Using The Blockchain," University of Saskatchewan, 2017.
[24] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from Internet voting to blockchain voting," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyaa025, Jan. 2021, doi: 10.1093/cybsec/tyaa025.
[25] Y. C. Loke, N. K. Batcha, and N. Ab Ziz, "Blockchain-Enabled Election Voting System," *Journal of Applied Technology and Innovation (e-ISSN: 2600-7304)*, vol. 4, no. 4, p. 51, 2020.
[26] R. Taş and Ö. Ö. Tanrıöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," *Security and Communication Networks*, vol. 2021, p. 6673691, Apr. 2021, doi: 10.1155/2021/6673691.
[27] H. Abdelatif, S. H. Abdelhakim, and S. Mustapha, "A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols." arXiv, Apr. 14, 2021. doi: 10.48550/arXiv.2104.07215.