Science Research Annals
A Scholarly Peer-reviewed Research Journal
Volume 14, No 1, Pages 42- 58, 2023
Available online at: http://journals.aaua.edu.ng/sra
ISSN: 2805 - 3508

Faculty of SCIENCE AAUA

Secured E-Voting and Results Transmission System using Blockchain Approach

D. A. AKINWUMI

Department of Computer Science, Adekunle Ajasin University, Akungba–Akoko, Ondo State, Nigeria

*Corresponding author E-mail address: david.akinwumi@aaua.edu.ng

A b s t r a c t

E-voting is a voting method where the electoral process is captured electronically. The challenges of the paper-based voting system such as fraud, delay in the operational processes and lack of transparency. Hence, the need for the development of e-voting system. Meanwhile, the issue of security such as authentication, confidentiality, integrity and transparency associated with this development remains a challenge. Many techniques have been proposed to tackle these challenges. However, blockchain technology have been discovered one of the prominent techniques to secure electronic and online systems. The objective of this research is to develop a secured e-voting system based on blockchain that uses both public and private key. The Rivest-Shamir-Adleman algorithm was used to generate the keys. The technology enables the voters to vote by using the private key and checks if the key is registered or not before creating and verifying a signature using the keys. The transaction is hash and recorded if the ballot is signed successfully without alteration in the chain making it immutable. The algorithm was implemented using a web voting system software with the use of Python libraries, Django python framework and PyCryptodome to prove the feasibility of the protocol. The system was deployed on Adekunle Ajasin University's network and experimental results demonstrated the ability of the system to verify and secure transactions in the chain. The results obtained was compared with results from the existing systems and showed a good performance. The system developed was found very suitable for securing votes and results transmission during any electronic electioneering process.

Keywords:

E-voting, Ballot, Blockchain, Security, Cryptography, Results transmission.

Accepted:27 June 2023

1. INTRODUCTION

Electoral process, voting inclusive is the process that allows the populace to choose their leaders and articulate views on how they will be governed. The veracity of democratic system is primary to the veracity of election itself (Shafi'í *et al.*, 2013). Electronic voting (e-voting) is a promising platform that is aimed at providing a secure, convenient, and efficient voting environment over the Internet. However, voting through the Internet introduces several concerns, such as fraud, anonymity, and abuse, among others. The crucial challenge for e-voting is the significant security risks it might cause. In order to reduce these risks, various protocols related to the ballot-privacy, individual verifiability, eligibility, completeness, fairness, uniqueness,

robustness, universal verifiability and receipt-freeness have been widely proposed.

Previous research has introduced different e-voting systems and protocols with different encryption schemes of varying complexity (Benaloh & Yung, 1982, Okediran *et al.,* 2011, Olaniyi *et al.,* 2012, Nakamoto, 2008). These systems make use of a combination of different protocols, such as blind signatures, threshold blind signatures, discrete logarithmic encryption, unstoppable channels, and anonymous channels or public bulletin boards, to satisfy the most properties that make e-voting systems secure.

Based on the common security requirements of participants, this paper proposed a blockchain-based protocol associated with the priorities of the ballot-privacy, verifiability, eligibility, completeness, uniqueness, robustness, and coercion- resistance. A prototype system was developed to verify the feasibility of this protocol, by implementing a real-life online voting website, which allows participants to vote and view the results easily.

2 LITERATURE REVIEW

Electronic voting systems depend on some electronic technology for their proper functionality. Traditional electoral procedures involving casting and hand counting paper ballots. The paper-based voting system consists of a voter manually marking the paper ballot and then the ballot being counted by hand by election officials. In elections using electronic voting systems, the processes are automated electronically. Many different technologies can be used to support the electoral process. This work focuses on block chain technology that will assist voting, counting and electronic transmission of votes.

The election data is communicated through one or more communication channels. For example, in the recent general elections in Nigeria, e-voting is physically supervised by the Independent Electoral Commission (INEC) using Bimodal Voter Accreditation System (BVAS) machines at polling units. The BVAS is an electronic device designed to read Permanent Voter Cards (PVCs) and authenticate voters (Wahab, 2022). Unfortunately, this drew much criticism because it was arguably acknowledge that there are many reported problems associated with the use of the BVAS machine.

In view of the this challenge, there is the need to build a system that support some form of voter verified printed audit trail with a risk-limiting audit or manual recount (Lindeman & Stark, 2012). Hence, a secured e-voting and results transmission system using blockchain approach is proposed. The system permits the voter to record a vote without having to be physically present in a supervised environment. This system adopts Remote Electronic Voting (REV). The components of the e-voting system and its architecture is presented in Figure 1 and Figure 2 respectively.

2.1 Components of the e-voting System

The e-voting system allows the voters to cast their vote from internet connected mobile device or a computer anywhere. Voter's login to the specified website and their identity is authenticated. The voting process then follows. Once the voting process is completed, the user logs off from the system. The e-voting system comprise of database, server, Encryption and Decryption algorithms and the tallying and result Consolidation. The database houses the voter's data such as Name, Age, and Telephone Number etc. The server is responsible for authentication of the voter based on the information supplied by the voter.

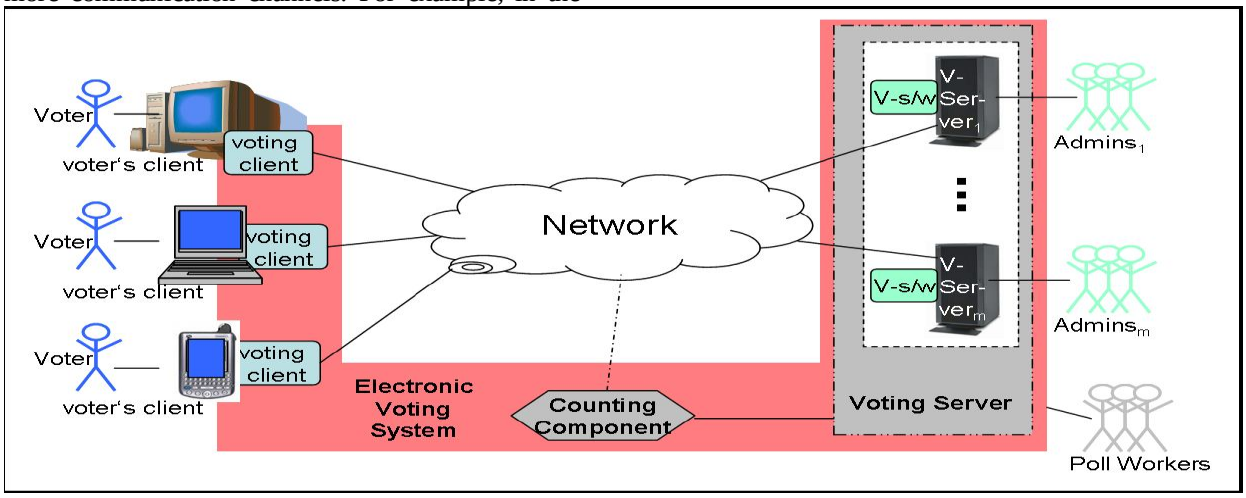


Figure 1: Components of the e-voting System (Volkamer & Krimmer, 2006).

A set of protocols that aids in Encrypted communication by using a chain of proxy servers take in messages, shuffle and send them randomly to the next destination. The messages is decrypted by using private key and the message order is shuffled by the node and transmits the result to the next node. The completion of voting process is followed by result consolidation after the tally process of votes. However, the issue of technical challenges need to be addressed.

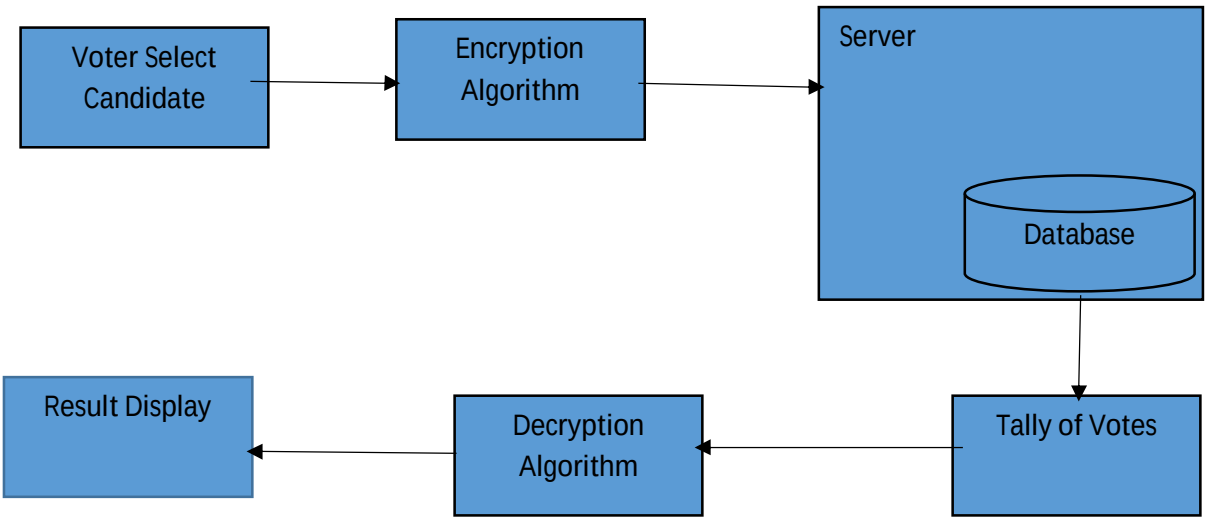


Figure 2: E-voting System Architecture (Laxmi, 2022)

2.1.1 Challenges of E-voting

This research work attempts to address some of the technical issues which most of the deployed e-voting systems around the world had not adequately addressed. Most of the challenges posed are majorly with respect to security, verifiability, dependability, anonymity and trust.

2.2 Related Works

Several related research works on electronic voting have been carried out in the research community; some of them are highlighted in this section.

The authors in Hirt & Sako (2000), proposed a homomorphic ElGamal encryption technique to design a private channel protocol with receipt-freeness. The authors were motivated to analyze the security of the multi-authority voting protocol and presented a novel generic construction for introducing receipt-freeness into a voting scheme by assuming some additional properties of the encryption function. The additional properties of the encryption function are random re-encryptability, existence of a 1-out-of-L re-encryption proof, existence of a designated-verifier re-encryption proof. The weakness of this protocol is that it doesn't suit a large-scale election.

The authors in Czepluch *et al.* (2015), discussed the application domains of the block chain and argued that block chain can be used for the e-voting. The purpose of the paper was to explore drawbacks and benefits of using block chain technology in application areas where transparency and trust-freeness advantageously can

be used. The author explained how Ethereum block chain can be used to deal with some voting security like storage insecurities, man in the middle attacks. Counting of votes are easily automated because it greatly reduced the work and time needed before a result is clear, while at the same time removing human errors, simplify the process of voting, anonymity of the voters is achieved if block chain technology is used. However, it was not implemented in the paper.

The authors in Zhao & Chan (2015), proposed a way to vote using Bitcoin and zero-knowledge succinct Non-interactive argument of knowledge (zk-SNARKs) with the properties named privacy, verifiability and irrevocability. The authors designed protocols for the bitcoin voting problem, in which there are n voters, each of which wishes to fund exactly one of two candidates A and B. The winning candidate is determined by majority voting, while the privacy of individual vote is preserved. Moreover, the decision is irrevocable in the sense that once the outcome is revealed, the winning candidate is guaranteed to have the funding from all n voters. We also use zero-knowledge-proofs, which, loosely speaking, allows one party to prove the correctness of a statement to another party, without revealing additional information. One major threat to the bitcoin network is caused by signature malleability. It means that one (users and miners) has the ability to alter a transaction's signature in away such that: (1) it

is still valid, and (2) the hash of the transaction changes.

The article in Okamoto (2003), uses a non-anonymous channel, a private channel and the bulletin board to propose a voting scheme, which satisfied receipt freeness and fairness property. The objectives are fairness, privacy, anonymity and receipt-freeness requirements. The participants of the scheme are the voters and voting commissioners (administrators, privacy commission members, and timeliness commission members). There are four stages to this scheme: the authorizing stage, voting stage, claiming stage, and counting stage. A voter performs just one round message exchange with the administrators in the authorizing stage, and is required to send just one message in the voting stage. Unfortunately, this protocol has been proved does not satisfy with receipt-freeness.

The paper in Chaum (2000), used an anonymous commutation channel to encrypt the ballot. The author used a technique based on public key cryptography that allows an electronic mail system to hide who a participant communicates with as well as the content of the communication in spite of an unsecured underlying telecommunication system. The technique does not require a universally trusted authority. One correspondent can remain anonymous to a second, while allowing the second to respond via an untraceable address. The shortfall of the technique is that the system can be compromised only by subversion or conspiracy of all of a set of authorities.

The work in Fujioka *et al.* (2010), proposed a practical secret e-voting scheme (FOO) used for the large-scale elections, which can ensure the privacy of voters and the fairness of voting. The scheme used the blind signature to blind the message the voter used to vote and send it to the administrator. In this scheme it also has its weakness, it requires all voters must vote and once someone abstains from voting, the result can tamper. The administrator cannot find out who tamper the result. This scheme couldn't provide receipt-freeness and public verifiability.

The article in Cohen & Fischer (2002), proposed a cryptographic protocol, which can hold a secure ballot election in which all communication is public. Since Cryptographic techniques are becoming important for a wide variety of distributed computing tasks where the processing agents are either unreliable or untrustworthy. The protocol encrypts the ballot by using homomorphism theorem and the government will release the tally result and a proof of its correctness, which can be verified by all. The probabilistic polynomial time algorithms were used as a proof to find solution to certain number-theoretic problem, for example if a set of conspiring voters (not including the government) can obtain more than a small epsilon advantage at compromising the privacy of the honest voters. The Government's ability to read any vote is a limitation using this scheme.

The paper in Pavel & Hitesh (2017), discussed the future of e-voting in relation to security and anonymity principles. The authors used a more secured platform (blockchain) called Zcash which is finally possible to tackle anonymous issues of blockchain transactions, which would open a possibility for blockchain voting. Since Ethereum has offered the smart contract functionality, the much-needed anonymity factor has not been present, so its integration with Zcash will most likely come up with the protocol, suitable for widespread, cheap voting system. The limitation of this paper is that the future Ethereum aims to make use of zk-SNARKs to add privacy and anonymity of transaction, The zk-SNARKs are complex to implement efficiently due to the time taken to generate proofs, which is one of the issues in implementing these today. However, steps towards adoption of zk-SNARKs have already been taken by Ethereum (Hudson, 2017).

The work in Patrick *et al.* (2017), presented a smart contract implementation for the open vote network that runs on Ethereum. The execution of the protocol is enforced using the consensus mechanism that also secures the Ethereum blockchain. The authors used two smart contracts that are both written in Ethereum's solidity language. The first contract I called the voting contract. It implements the voting protocol, controls the election process and verifies the two types of zero knowledge proofs we have in the open vote network. The second contract is called the cryptography contract. It distributes the code for creating the two types of zero knowledge proofs. This provides all voters with the same cryptography code that can be used locally without interacting with the Ethereum network. However, some difficulties were faced while implementing the open vote network on Ethereum which are lack of support for cryptography, call stack issues, lack of debugging tools, mitigate loss of voting key, maximum number of voters.

The authors in Freya *et al*. (2018), proposes an e-voting scheme based in blockchain technology that meets fundamental e-voting properties whilst, at the same time, provides a degree of decentralization and places as much control of the process in the hands of the voters as was deemed possible. The protocol utilizes the blockchain to store the cast ballots, therefore in this context the blockchain acts as a transparent ballot box. Each voter will be a peer i.e. a node in a network of equals. Every voter will be responsible for making sure that fraudulent votes are rejected, hence that consensus is maintained according to the election rules. Since the Central Authority (CA) is the only centralization point of the protocol and it is assumed to be trusted. However, if

the CA breaks that trust in the current setting, it could arbitrarily cast votes for voters that have not voted.

In Tohari *et al.* (2019), an Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography was developed**.** The authors observed that existing mobile voting scheme solution uses symmetric encryption algorithms or hybrid symmetric and therefore present a novel mix-type remote voting system that permits verifying the correctness of a voting process without requiring complex and costly zero-knowledge proofs. However, the system needed more security tools to withstand attacks. For example, packet sniffing, key logging attacks, brute force attacks.

In the work Khan *et al.* (2020), the authors developed secure digital voting system based on Blockchain Technology. The existing digital voting security system lacks wide spread acceptance, because data loss through identity theft and low latency. The research aimed to improve the overall resilience of e-voting systems by designed scheme conforms to the fundamental requirements for e-voting schemes. The design use Multichain platform and presents in-depth evaluation of the scheme, which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme. However, the scheme only focused on improving the resistance of blockchain technology to 'double spending' problem that results to 'double voting'.

In the work Arthur *et al.* (2021), a Cloud based e-voting system using Information Dispersal Algorithm (IDA) is presented. The existing schemes lack adequate security from malicious activities such as hacking and hijacking. In the IDA approach, upon voting, the voters vote record is encrypted and split for distribution on several virtual cloud servers. At the end of the voting period, the split vote records are reassembled into their original state for counting to take place. The system represents the voters vote record in a secured manner that could not be easily accessed by hacks and exploitation while the voting process is on- going. However, there is the need to improve on the system to be able to identify and thwart possible intrusions. In Ali *et al.* (2022), an efficient electronic voting system in a cloud computing environment using Elliptic curve cryptography (ECC) was developed. There were challenges of vote confidentiality, vote integrity and vote stuffing face by existing cloud-based e-voting systems. The developed e-voting system s based on Homomorphic encryption to ensure privacy, confidentiality and integrity of vote in the cloud. However, the system lack biometric and digital signature authentication processes which makes easy to compromise.

I want to appreciate these authors for their contributions to knowledge, however, integrity of votes is still the challenge of most the existing schemes reviewed. The limitations observed in the works serve as motivation for this research. The contribution of this work is the immutability of votes, which ensures the integrity of all votes cast during the election and transmission of results leveraging on the strength of blockchain technology.

3. THE PROPOSED SECURED E-VOTING SYSTEM BASED ON BLOCKCHAIN

The conceptual diagram of blockchain based e-voting system is presented in Figure 3. The system is divided into four phases. The first phase is the preliminary registration phase, which comprises of registration and authentication of voters and candidates, generation of public keys and private keys. The second phase is the voting phase where voters perform their civic duties during election. The third phase is the tallying or matching phase that is available for the public for the counting of votes. The fourth phase is the verification phase for the verification of votes. Transactions with valid data will be generated and also be backed-up into another node for recovery, they are then sealed into blocks, after that, transactions and blocks can be explored. Tampered records can then be identified and verified. Blocks can be synchronized back to the back-up node.

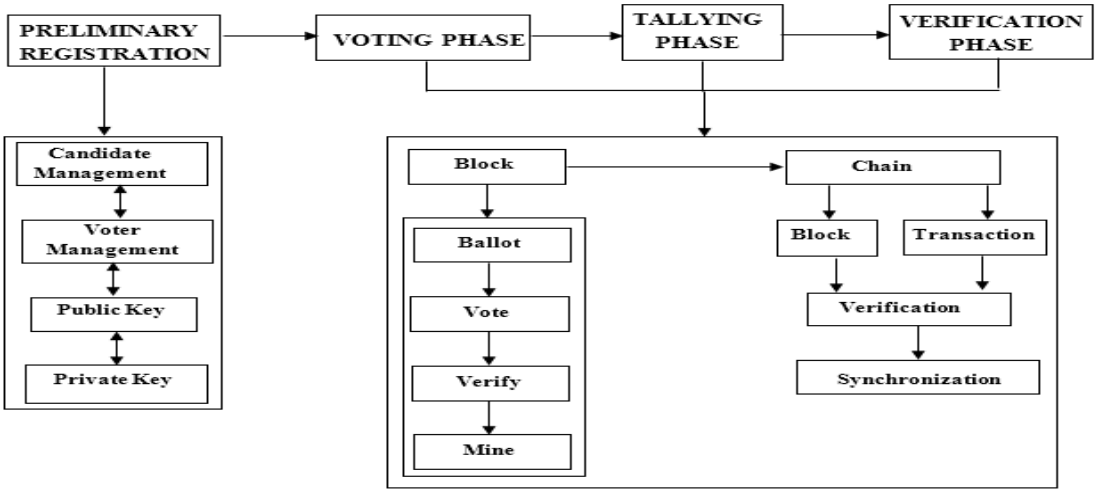


Figure 3: System Architecture of Blockchain based E-voting System

3.1 Voting Logic Workflow

Before the voting phase, incoming new registration requests are no longer accepted. The voters use their private key to sign favorable candidate, they will get a unique signature using the private key and the signature is then verified using the public key. The voting logic workflow is shown in Figure 4.

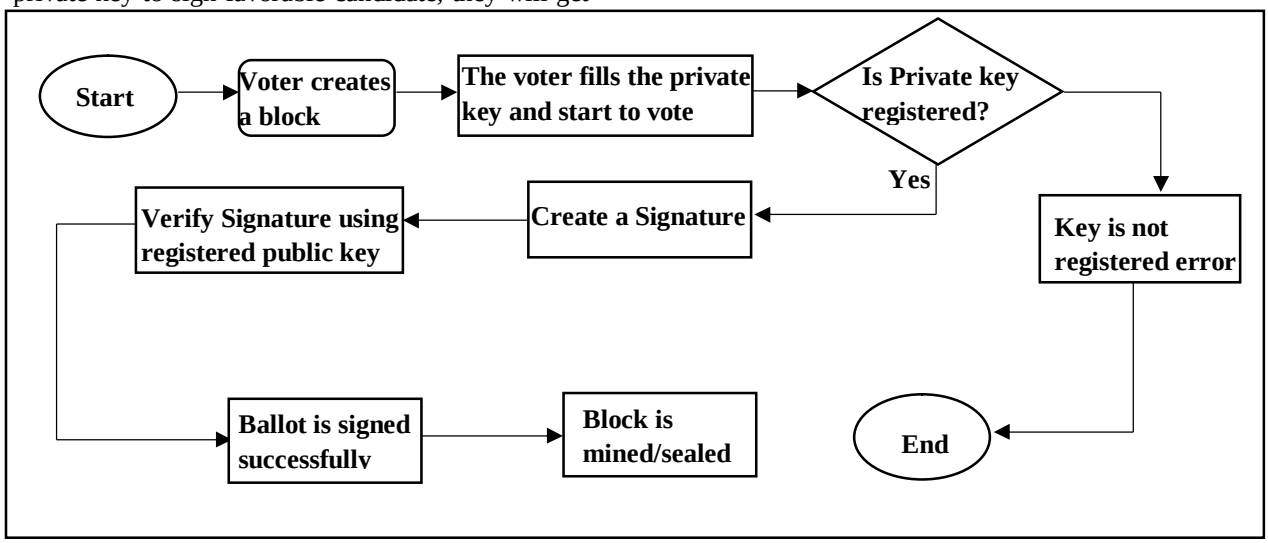


Figure 4: Voting Logic Workflow (Digital Signature Flow)

As earlier discussed, a set of protocols that aids in encrypted and decryption using public and private keys are deployed. A secured protocol efficient for encrypted and decryption is the Rivest-Shamir-Adleman (RSA) algorithm.

3.1.1 Rivest-Shamir-Adleman (RSA) Algorithm

RSA algorithm is a type of public key cryptography, which is used to encrypt and decrypt the messages. This type of public key cryptography is based on the Integer factorization problem, where the multiplication of two large prime numbers is easy, but it is difficult to factor it (the result of multiplication, product) back to the two original numbers. Its security is based on the difficulty of large integer decomposition. The RSA key pair can be generated as described below:

1. **Modulus generation**:
   i. Select *p* and *q*, which are very large prime numbers
   ii. Multiply *p* and *q*, *n=p, q* to generate modulus *n*
2. **Generate co-prime**:
   i. Assume a number called *e*.
   ii. *e* should satisfy a certain condition; that is, it should be greater than *1* and less than *(p-1) (q-1)*. In other words, *e* must

be a number such that no number other than *1* can divide *e* and *(p-1) (q-1)*. This is called **co-prime**, that is, *e* is the co-prime of *(p-1) (q-1)*.

3. **Generate the public key**:

The modulus generated in step 1 and co-prime *e* generated in step 2 is a pair together that is a public key. This part is the public part that can be shared with anyone; however, *p* and *q* need to be kept secret.

4. **Generate the private key**:

The private key, called *d* here, is calculated from *p*, *q*, and *e*. The private key is basically the inverse of *e modulo (p-1) (q-1)*. In the equation form, it is this as follows:

$$ed = 1 \bmod (p-1)(q-1)$$

3.1.2 Encryption and decryption using RSA

RSA uses the following equation to produce cipher text: $C = P^e \bmod n$

This means that plaintext *P* is raised to *e* number of times and then reduced to modulo *n.*

Decryption in RSA is provided in the following equation:

$P = C^d \bmod n$

This means that the receiver who has a public key pair (*n, e*) can decipher the data by raising *C* to the value of the private key *d* and reducing to modulo *n.*

3.2 Chain Simulation Workflow

Transactions (ballots) with valid data will be generated into two nodes (real node and back-up node). Data to be generated randomly are the block header and block body. The block header, which is composed of id, vote, timestamp, nonce block_id, Merkle root and the data are then backup into another node for restoration after an attack. The block body contains transactions. Previous transactions are then deleted before generating new transactions. After randomly generating new transactions that are up to 10,000 records, the transactions are then verified. The system checks the private keys used in voting for each transaction and the system creates signatures if keys are correct. The transactions verification is done after which the system verifies the signatures by checking if the public keys of the corresponding private keys of each transaction exist in the system. Blocks are created, linked together, mined (sealed) to occupy the transactions. The transactions are sealed into the blocks, the blocks are linked together to form a chain of blocks that can't be alter. The blocks are mined by generating a valid hash algorithm for each block. The chain simulation logic workflow is depicted in Figure 5.

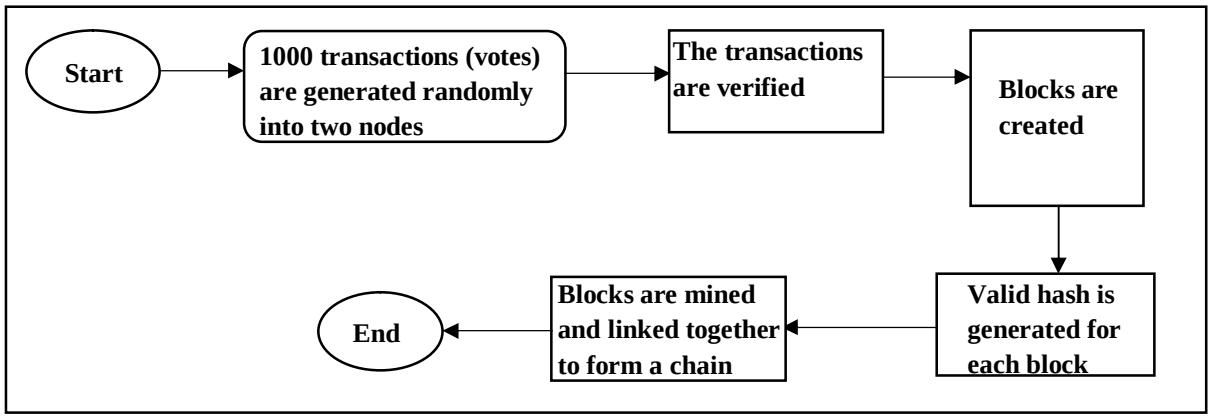
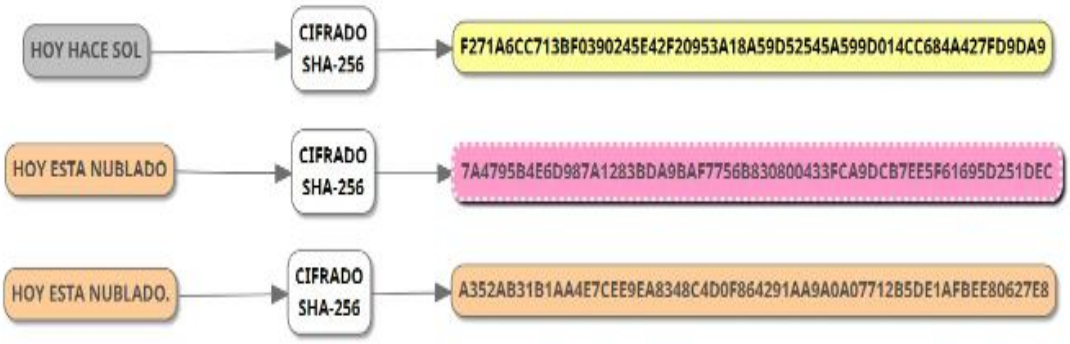


Figure 5: Chain simulation workflow

3.2.1 Hash Algorithm

Hashing is the process of scrambling a piece of information or data beyond recognition. We use hash functions to convert input into hash digest. A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. Three properties make SHA-256 this secure. First, it is almost impossible to reconstruct the initial data from the hash value. A brute-force attack would need to make 2^{256} attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2^{256} possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small. Finally, a minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this is known as the avalanche effect.



4. EXPERIMENTAL SETUP

The experimental setup was done using a LAN to monitor network traffic flow. The hardware components used in the development of the proposed system are: HP Speare Laptop with Intel® Core (TM)2 Duo processor and 4 gigabytes of RAM. Windows 7 Operating System manages computer hardware, software resources, and provides common services for computer programs. Programming language used is Python 3.8.2 with the following python libraries; System (sys), Django Template tags, Django-crispy-forms 1.9.0, Pycryptodome 3.10.1, Merkle Tree, Virtualenv 20.0.15, RSA 4.7.2, Django 3.0.4 as the framework for the backend. For the frontend, Hypertext markup language (HTML), Cascading Style Sheets (CSS), JavaScript (JS), Bootstrap 4 and Sqlite3 for the database.

4.1 Test Bed Setup

The research was conducted using the network of Adekunle Ajasin University, Akungba-Akoko, Nigeria as the test bed. In the Experimental setup, fifty (50) computers of the University E-learning Centre with the above hardware configuration were connected. The first computer runs the Server Application while the other computers runs the Client Application. The computers were all connected together on a LAN. The Algorithm was implemented on Internet connection bandwidth of 40 megabytes per second (Mbps), for the conduct of student Union elections.

4.2 System Implementation, Results and Discussions

A web application was developed to simulate our ideas. The first process is the registration of both the voters and candidates which can be seen once the url is been accessed using the browser. If the registration or sign up is successful, the voter is expected to login into the system. Login information (username and password) is authenticated and error returned if failed. If the login is successful, it takes the voter to the home page as presented in Figure 6. The Voting page presented in Figure 7 creates and submits ballot after which the voter must have provided the candidate choice number and his/her private key. The private key was generated from the public key using RSA algorithm and held privately from the public. Once signature is created and verified using the public key (saved on the system) of the private key. The private key entered in the voting page has been verified. The ballot is successfully signed after verification. The ballot-sealing page in Figure 8 mines the block (ballot). The block is encoded and the encoded block is then hex using SHA3_256 hash function. The requirement level is checked and if it's true, the ballot is hashed (sealed). Figure 9 shows how the block is being hashed. The block detail page in Figure 10 shows the previous hash of the previous block, the transaction hash and block hash of the current block, the nonce and timestamp that the transaction data existed when the block is published in order to get into its hash. The chain section of the e-voting system which can be clicked in Figure 6 displays the simulation of blockchain based e-voting system. In Figure 11, 1000 transactions(votes) are generated randomly. Figure 12 shows the list of unconfirmed votes. The transactions are mined into blocks after succesful signature and key verification as depicted in Figure 13. After the transactions are mined into blocks, the votes(transactions) are now confirmed as shown in Figure 14. Figure 15 shows the list of blocks that can be verified and synchronize.In Figure 16, the tampered blocks and trasactions are shown. In Figure 17, the blocks that has been tampered with is seen via the command prompt and is being reverted back to the deafult numbers of transactions from the onset in Figure 18.

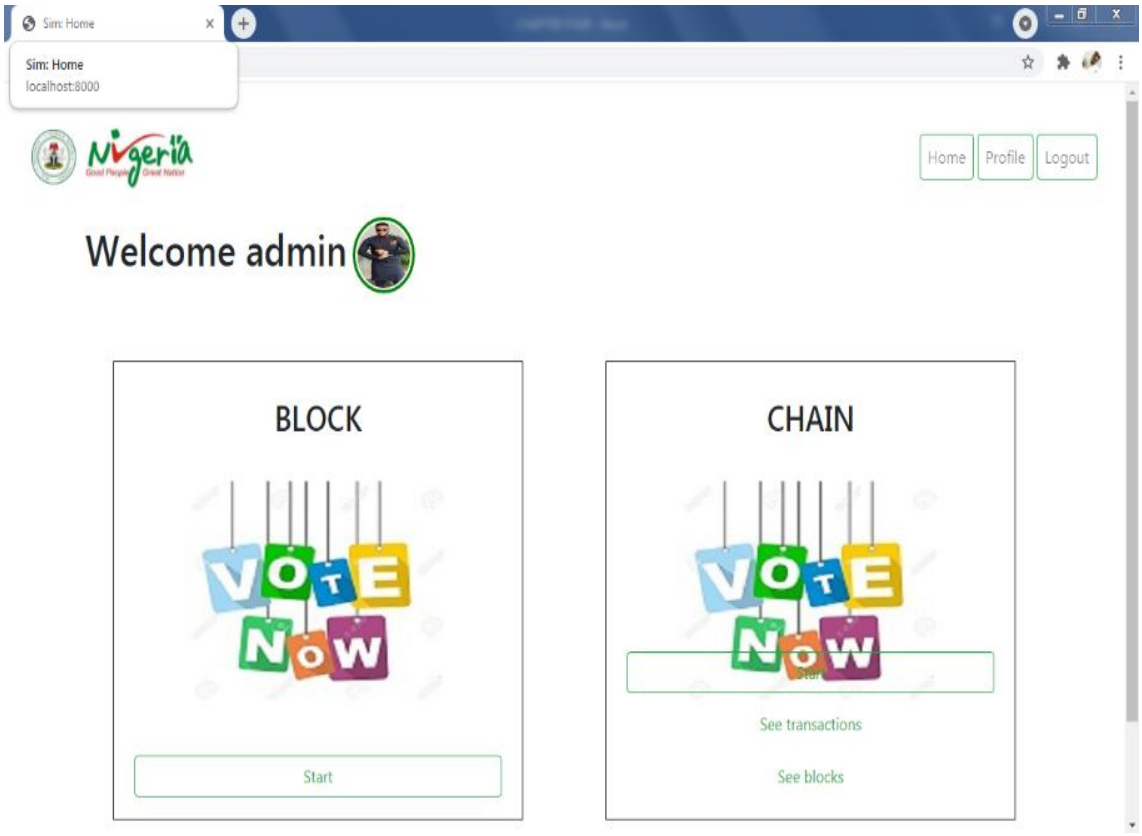


Figure 6: Homepage

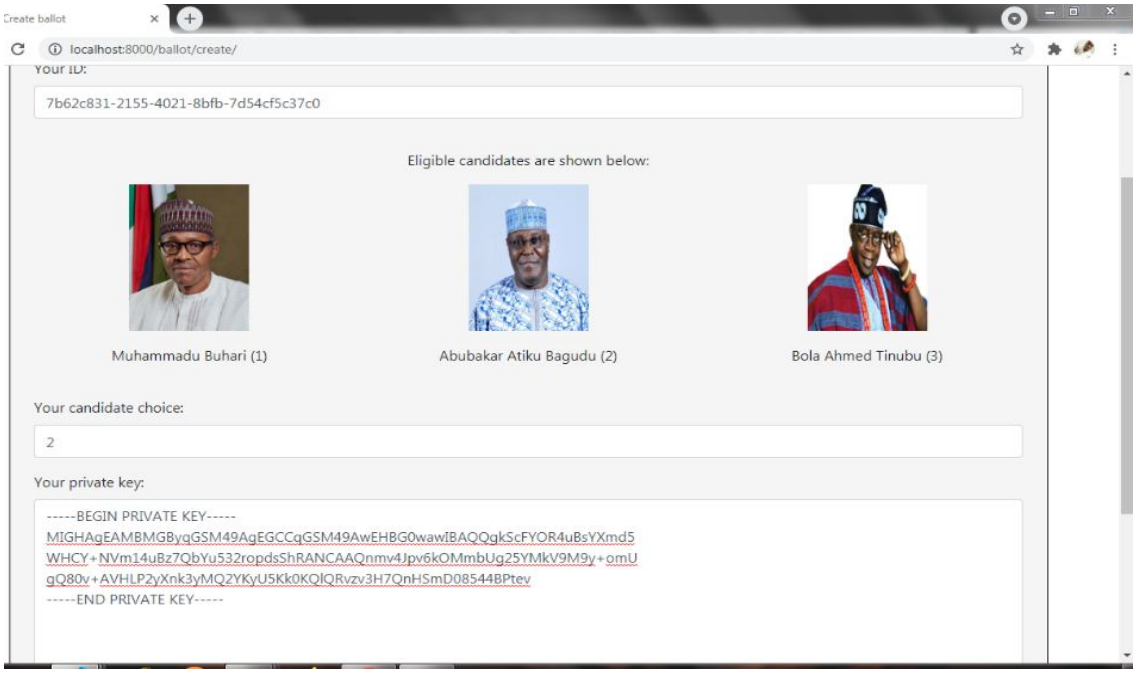


Figure 7: Voting Page

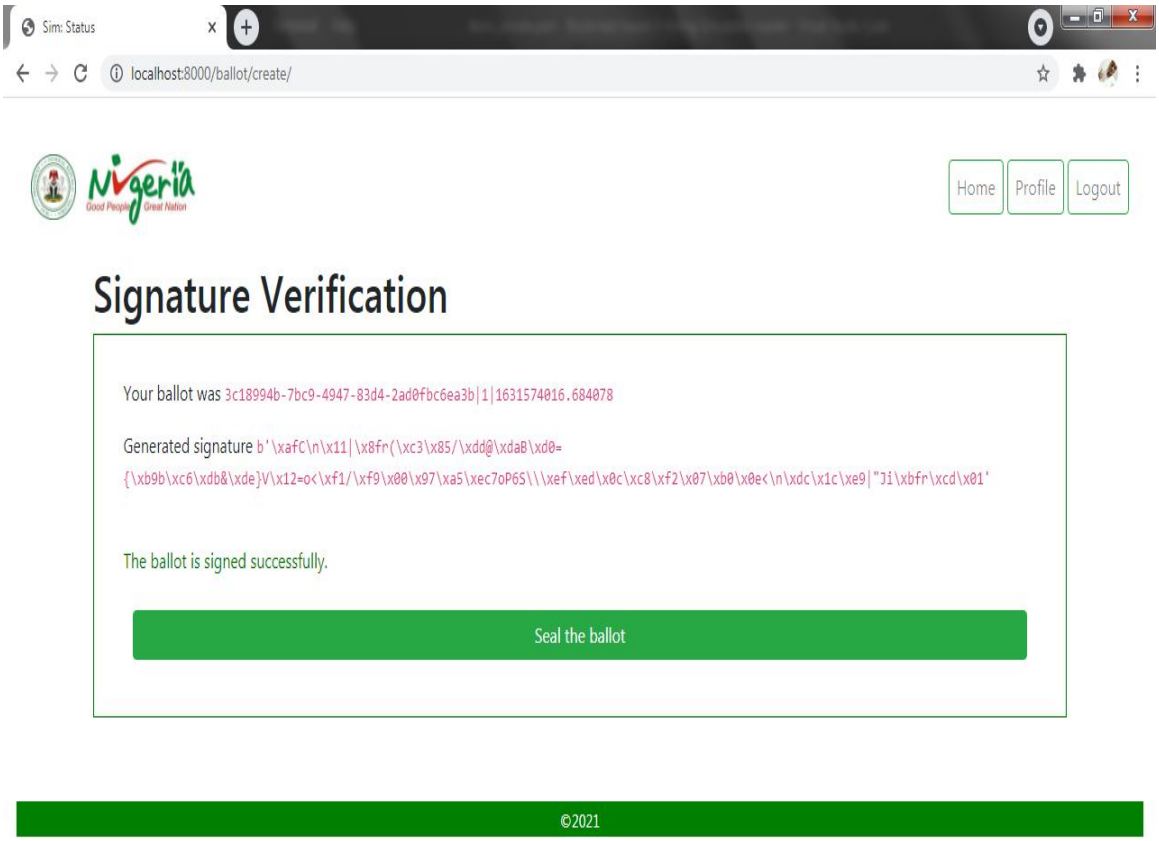


Figure 8: Ballot Sealing

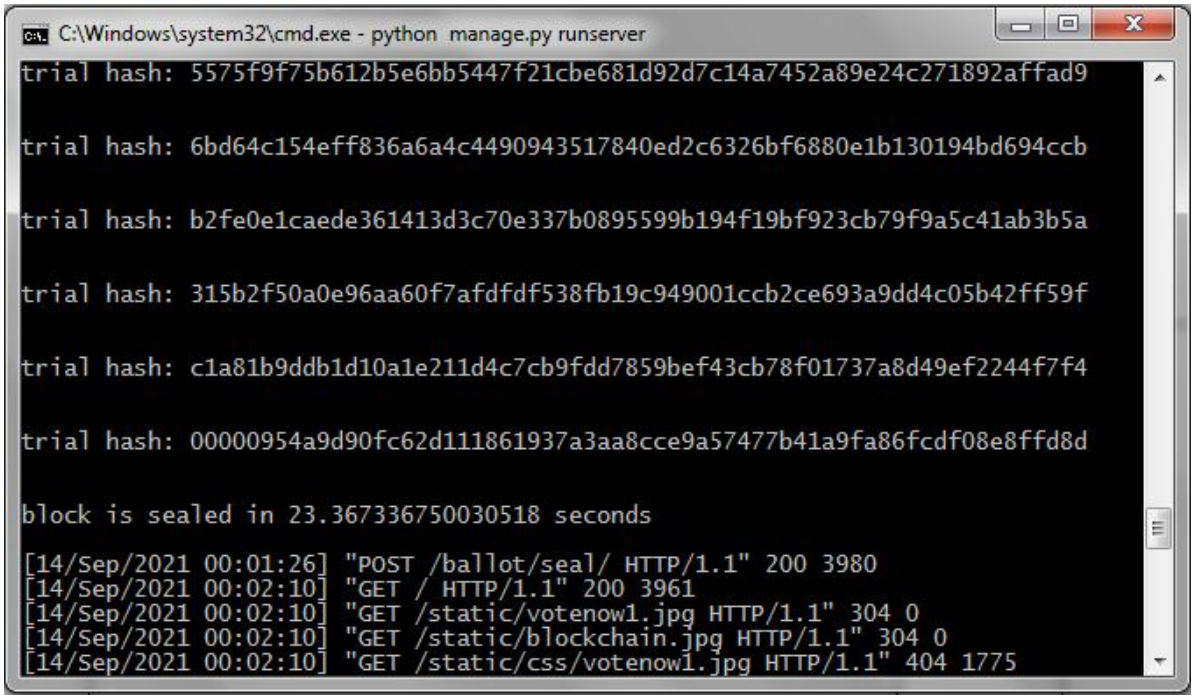


Figure 9: Block Hashing

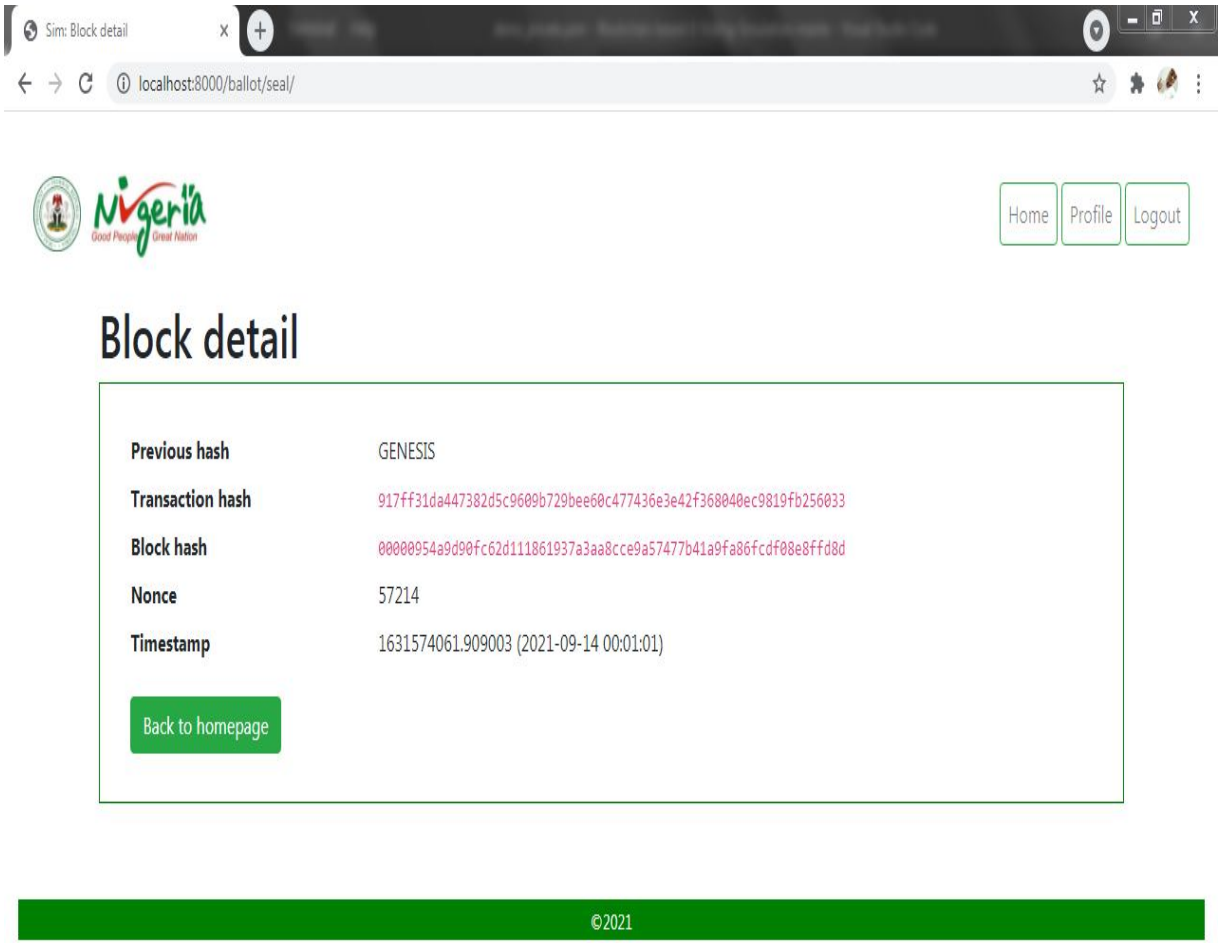


Figure 10: Block Detail

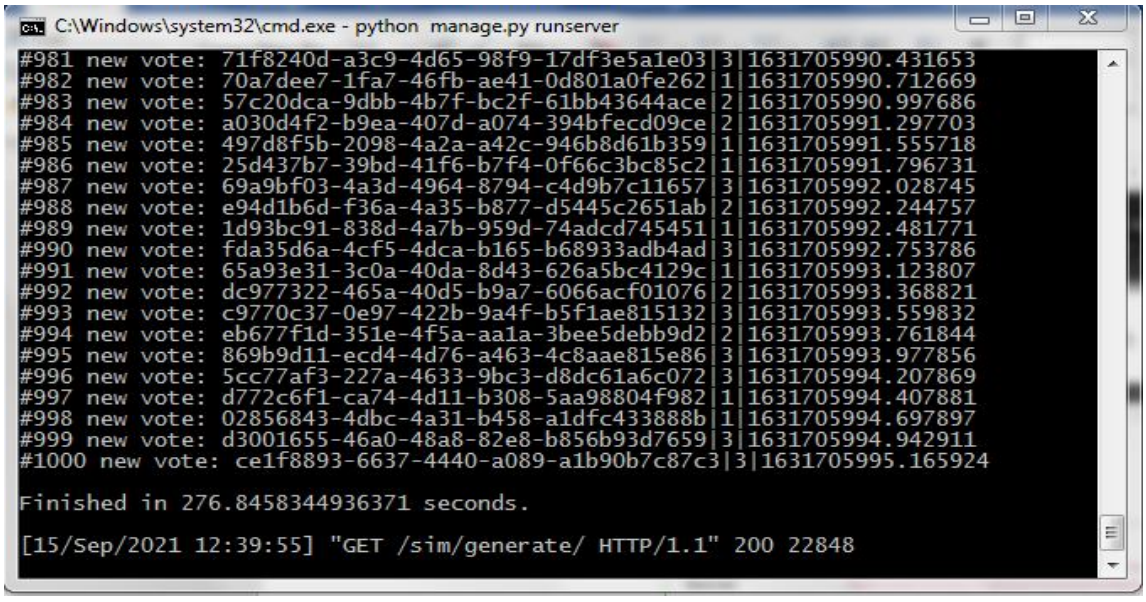


Figure 11: Votes Generation

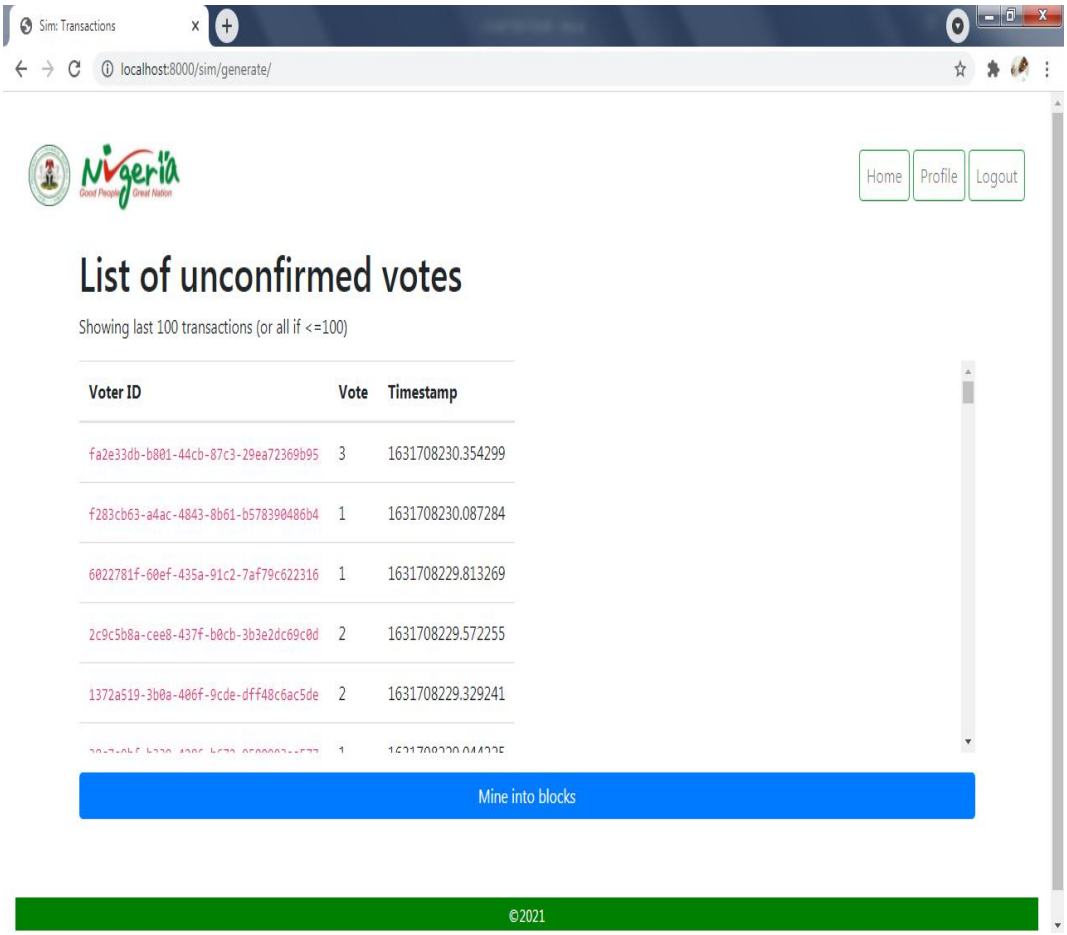


Figure 12: Unconfirmed Votes

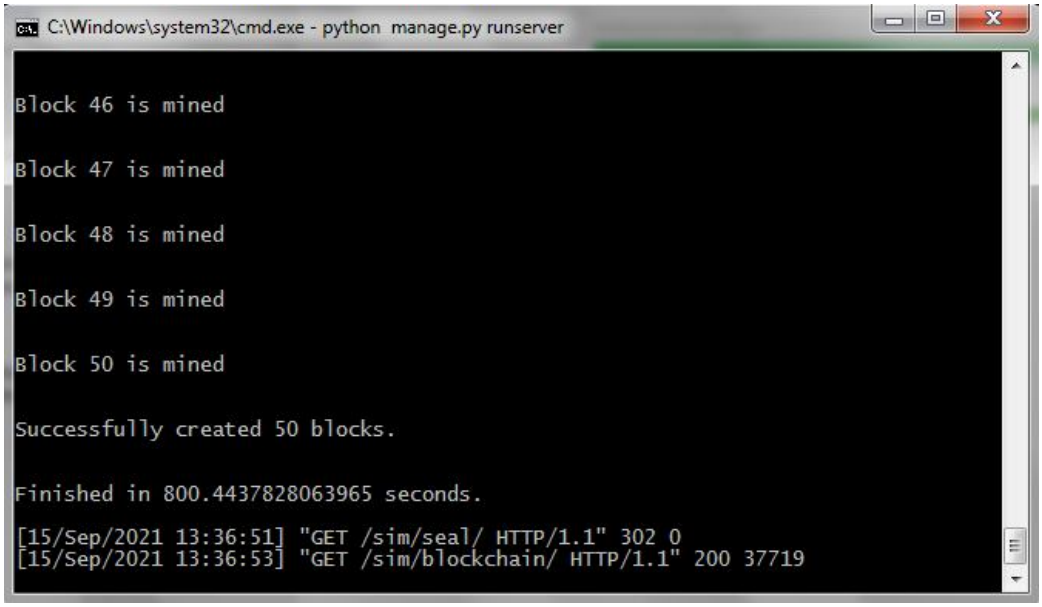


Figure 13: Block Mining

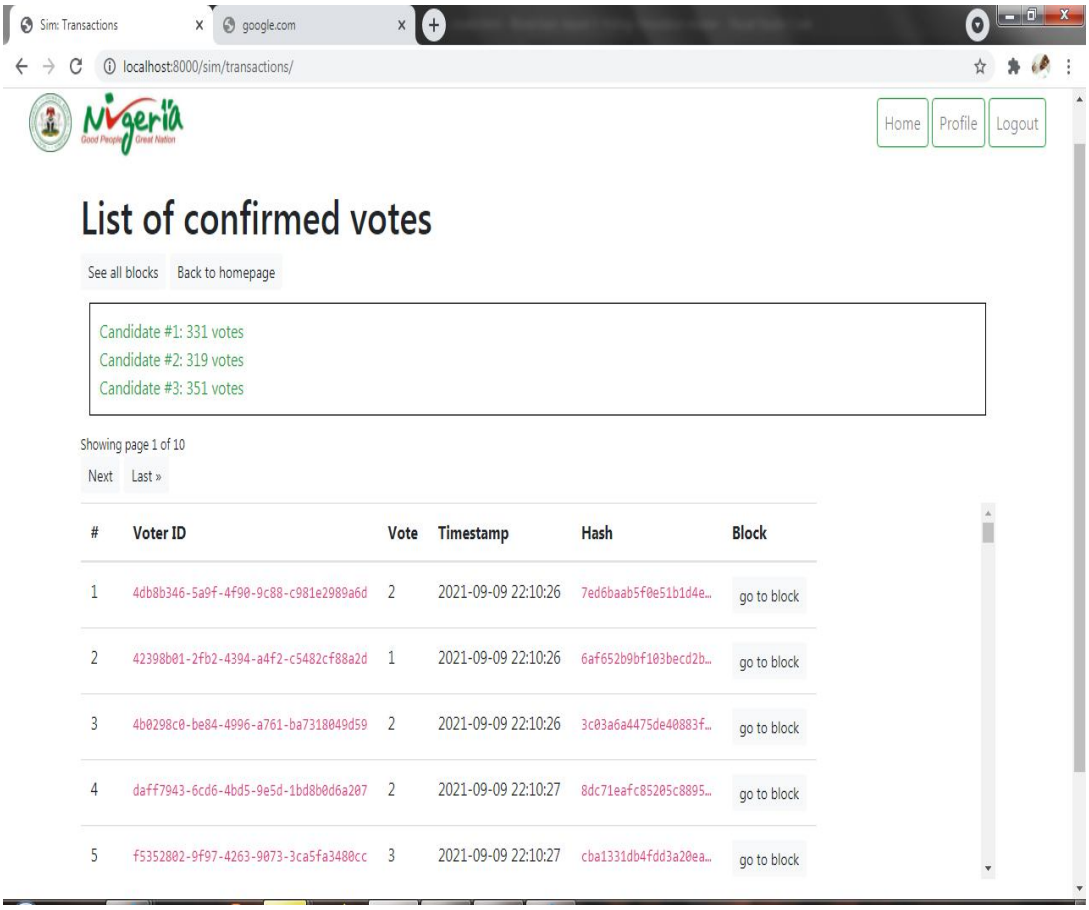


Figure 14: Confirmed Votes

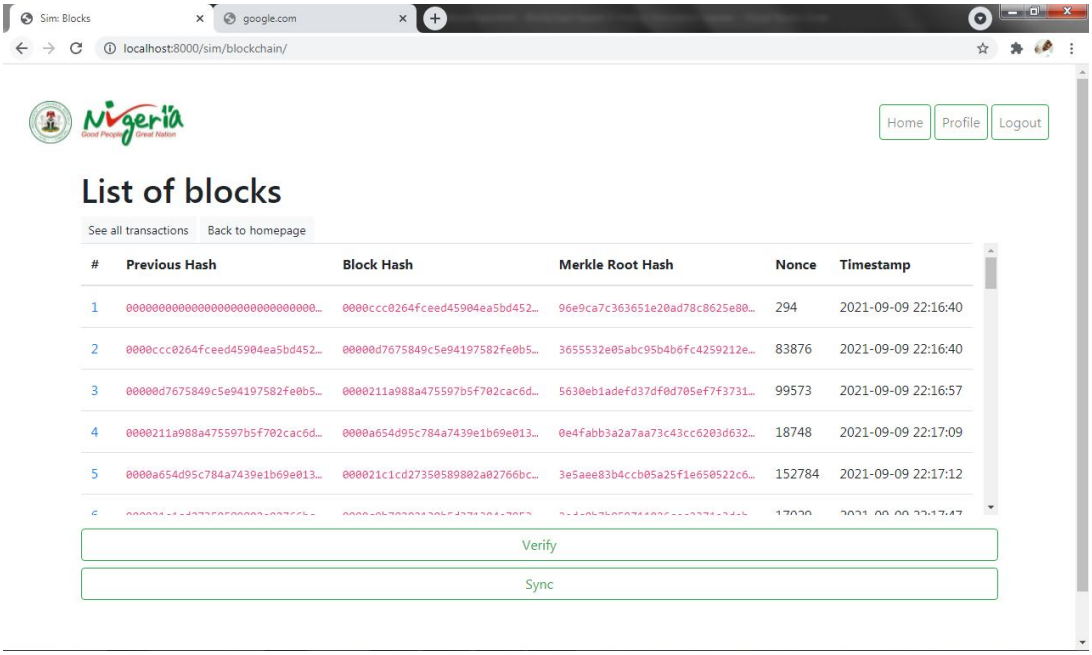


Figure 15: Blocks

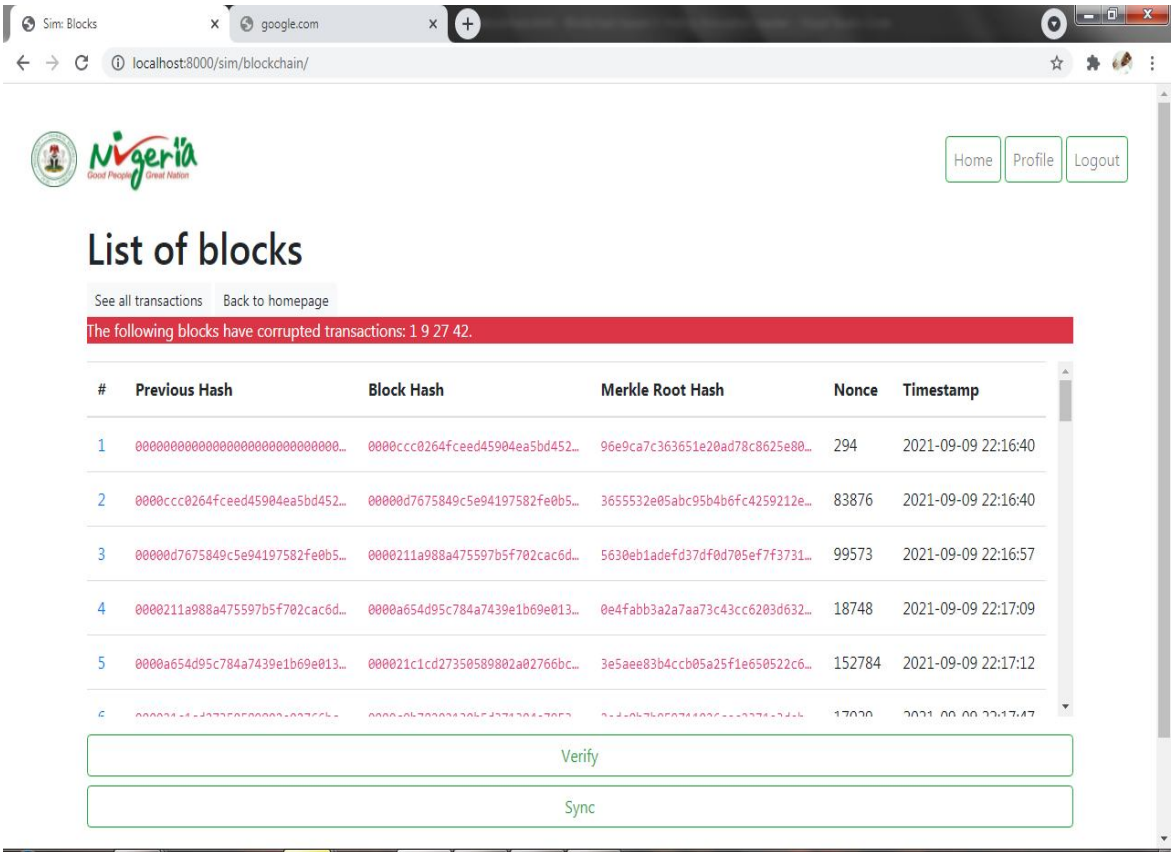


Figure 16: Tampered Votes

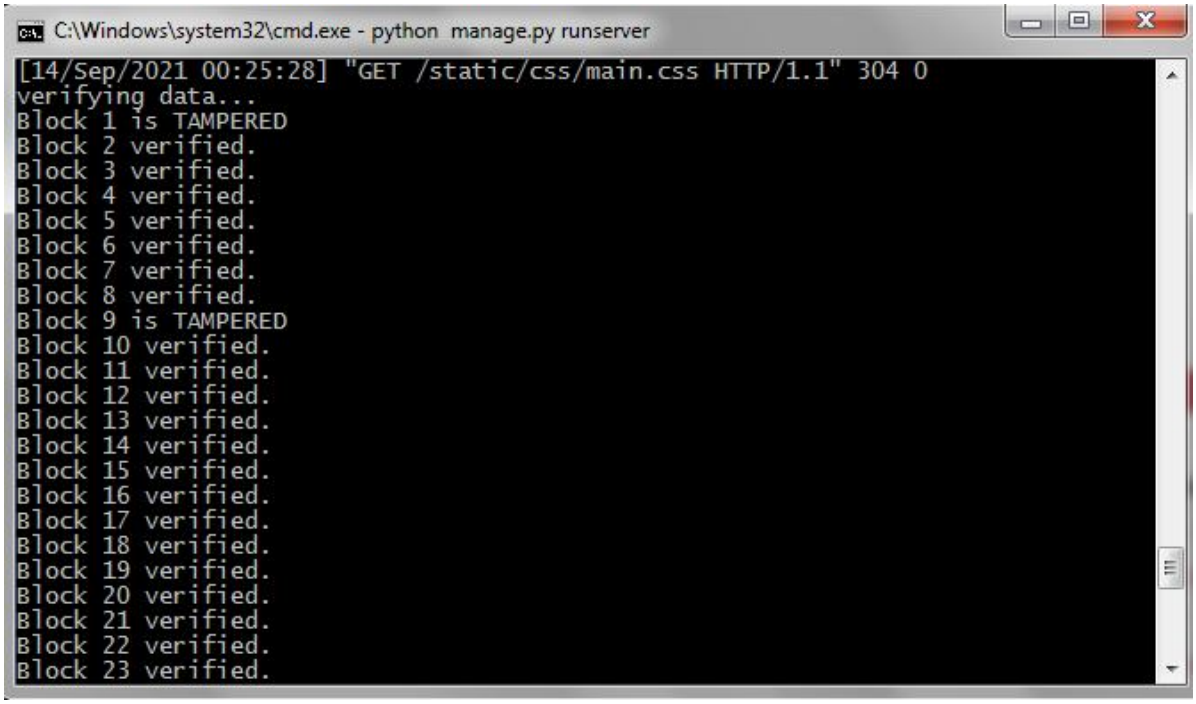


Figure 17: Blocks Verification

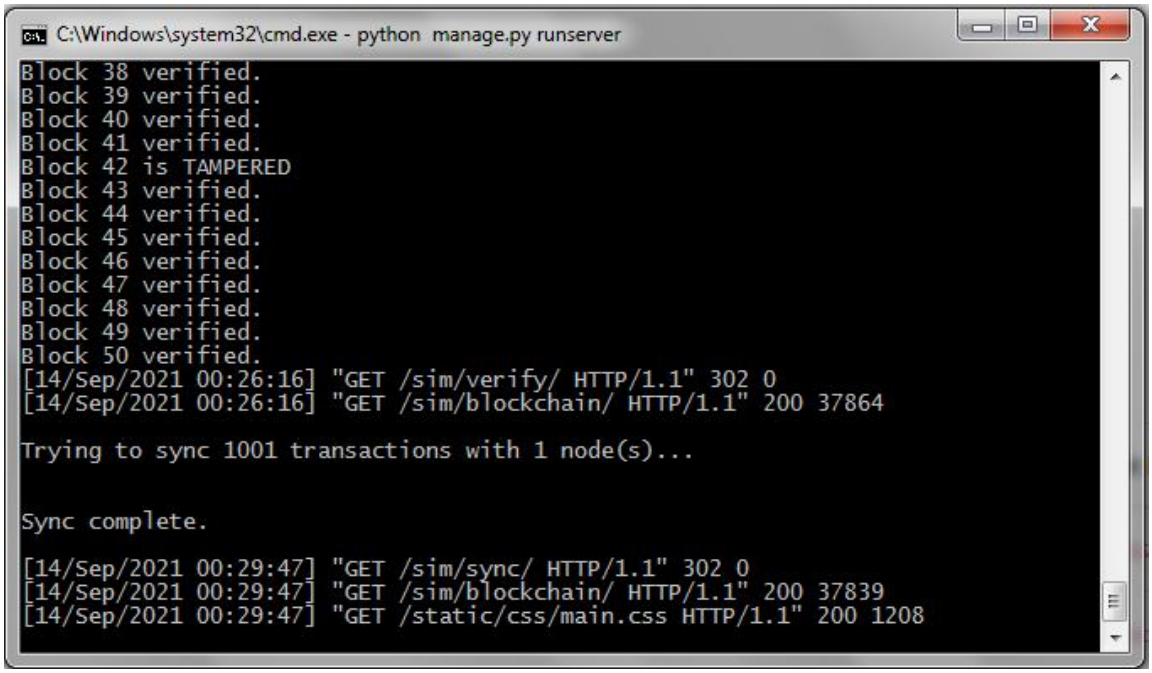


Figure 18: Synchronization

5. PERFORMANCE EVALUATION OF THE PROPOSED SYSTEM

In this paper, a secured e-voting and result transmission system using Block Chain is proposed. The performance of the proposed system was evaluated based on results obtained from case study of Student Union elections in Adekunle Ajasin University E-learning Centre's network.

Table 1 shows the quantitative comparative analysis of the proposed system with some other related existing works based on the following metrics: Privacy, Scalability, Accuracy, Uniqueness verifiability and Transparency.

.Table 1: Quantitative Comparison of the Proposed System with Previous Research Works

Desired Features/Functionality	Baudron *et al*, (2001)	Zhao and Chan, (2015)	Okamoto, (2003)	Jason and Yuichi, (2017)	Current Research
Privacy	0.30	0.30	0.30	0.20	0.30
Scalability	0.10	0.20	0.10	0.30	0.30
Coercion-resistance	0.30	0.20	0.10	0.30	0.20
Verifiability	0.30	0.30	0.30	0.30	0.30
Uniqueness	0.20	0.20	0.10	0.30	0.20
Transparency	0.10	0.20	0.20	0.20	0.30

Table 2 shows the qualitative comparative analysis of the system with some other related existing works. The evaluation was based on the following metrics: Ballot-Privacy, Scalability, Coercion-resistance and verifiability.

Table 2: Qualitative Comparison of the Proposed System with Previous Research Works

Desired Features/Functionality	Baudron *et al*, (2001)	Zhao and Chan, (2015)	Okamoto, (2003)	Jason and Yuichi, (2017)	Current Research
Ballot-Privacy	High	High	High	Average	High
Scalability	Not Scalable	Scalable	Not Scalable	Scalable	Scalable
Coercion-resistance	High	Average	Low	High	average
Verifiability	Verifiable	Verifiable	Verifiable	Verifiable	Verifiable

6. CONCLUSION AND RECOMMENDATION

This study present a secured e-voting and results transmission system using blockchain approach. The block chain architecture depict a secured model that seeks to automate the electronic electioneering process, through the cryptographic hash function and block to prevent attacks on the system. The introduction of e-voting has brought more risks because, the system is at the proximity of voters as well as hackers who are all out to discredit the integrity of the election or bring down the entire network. Therefore, fixing the issues through existing approaches is a challenge. The failure of many of the present approaches points to the need for a new and better approach. One of the prominent techniques to tackle this challenge is the use of blockchain technology. The primary advantage of this protocol is to guarantee the authenticity of electronic voting, as every ballot will be broadcasted to the blockchain once voting starts. Moreover, as blockchain is a decentralized public ledger, ballots result are represented in a real time and cannot be modified by an individual, which satisfies the design of open-auditing. This research proposed a block chain approach to secure e-voting and result transmission system so as to enhance free, fair and credible elections. The evaluation obtained from the results shows the adequacy of the system for e-voting. Future works would consider accomplishment of concurrent multiple voting.

7. ACKNOWLEDGMENTS

Thanks to the Academic staff and Technologist of the Department of Computer Science as well as staff of the E-Learning Centre at the Adekunle Ajasin University Akungba-Akoko, Nigeria, for providing the enabling environment for this research, and for allowing us carry out our experiments on their networks. I want to specially, acknowledge the contribution of my student Mr. Adebanji, Peter Adeyinka to this research.

REFERENCES

Ali, A., Zaid, K., Mustapha, H., Mostafa, B. & Mohamed, M. (2022). "An Efficient electronic voting system in a cloud computing environment using Elliptic curve cryptography (ECC)" *International Review on Computers and Software (I.RE.CO.S.),* 10(11).

Arthur, J. K., Kofi, S. A. & Charlse, A. (2021). "A Secured Cloud-based E-voting System using Information Dispersal Algorithm" *International Journal of Computer Applications 175(20):975-8887.*

Benaloh, J. C., & Yung, M., (1982). "Distributing the Power of a Government to Enhance the Privacy of Voters", 5th ACM Symposium on Principles of Distributed Computing, pp.52-62.

Chaum, D. (2000). "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM 2, 84-90.

Cohen, J. & Fischer, M. (2002). "A Robust and Verifiable Cryptographically Secure Election Scheme", Yale University. Department of Computer Science.

Czepluch, J., Lollike, N. & Malone, S. (2015). "The Use of Block Chain Technology in Different Application Domains", The IT University of Copenhagen, Copenhagen.

Freya, S., Apostolos, G., Raja, A., & Konstantinos, M., (2018). "E-Voting with Blockcahin: An E-Voting Protocol with Decentralisation and Voter Privacy", ISG-

SCC, Royal Holloway, University of London, Egham, United Kingdom.

Fujioka, A., Okamoto, T. & Ohta, K. (2010). "Practical Secret Voting Scheme for Large Scale Elections", In International Workshop on the Theory and Application of Cryptographic Techniques, Springer, pp. 244-251.

Hirt, M. & Sako, K. (2000). "Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Advances in Cryptology Eurocrypt, Springer, pp. 539-556.

Hudson, J. (2017). EIPs, GitHub Website, https://github.com/ethereum/EIPs.

Khan, K. M., Junaid, A. & Muhammad, M. K. (2020). "Secure Digital Voting System based on Blockchain Technology" *NED University Research Journal of Engineering and Technology.* 456 (13).

Laxmi, A. (2022). "How Electronic Voting (e-voting) Works – Types, Application and Advantage". http://electricalfundablog.com/electronic-voting. Access: March 4, 2022.

Lindeman, M. & Stark, P. B. (2012). A gentle introduction to risk limiting audits. IEEE Security & Privacy (5), pp 42–49.

Nakamoto, S. (2008). "Bitcoin; A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf.

Okamoto, T. (2003). "An Electronic Voting Scheme", In Advanced IT Tools. Springer, pp. 21-30.

Okediran, O. O., Omidiora, E. O., Olabiyisi, S. O., Ganiyu, R. A. & Alo, O. O. (2011). "A Framework for a Multifaceted Electronic Voting System", International Journal of Applied Science and Technology Vol. 1(4), pp 135 – 142.

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., Omotoso, A. & Ogungbemi, O. B. (2012). " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89.

Patrick, M., Siamak, F., & Feng, H., (2017). "A Smart Contract for Boardroom Voting with Maximum Voter Privacy", School of Computing Science, Newcastle University UK.

Pavel, T. & Hitesh, T. (2017). "The Future of E-voting", IADIS International Journal on Computer Science and Information Systems, Vol. 12, No. 2, pp. 148-165.

Shafi'í, M., Olawale, S., Damian, O. & Mohammed, D. (2013). "The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity", *I. J. Computer Network and Information Security*, 2013, 5, 9-18.

Tohari, A., Jianku, H. & Song, H. (2019). "An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography" *Third International Conference on Network and System Security, NSS 2019,* Gold Coast, Queensland, Australia, October 19-21, 2019.

Volkamer, M. & Krimmer, R. (2006). Ver-/misstrauen schaffende Maßnahme beim e-voting. In Christian Hochberger and Rüdiger Liskowsky, editors, INFORMATIK 2006- Informatik für Menschen, Volume P-93, Pages 418–425. Lecture Notes in Informatics (LNI).

Wahab, B. (2022). Everything to know about BVAS and how it'll be deployed for 2023 elections Pulse Nigeria, https://www.pulse.ng/news/

Zhao, Z. & Chan, H. (2015). "How to Vote Privately using Bitcoin", In International Conference on Information and Communications Security, Springer, pp. 82-96.