ISSN 2229-5518

Framework For Electronic Voting System Using Blockchain Technology

Banjo Oluwafemi[1]*, Awodele Oludele[2], Eseosa Ehioghae[3]

[1,2]Department of Computer Science, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

[3]Department of Software Engineering, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Abstract— A system with a porous electoral process will produce the wrong leadership. The quality of an election determines the quality of the selected leadership of a community, state, and nation at large. Over the years, different solutions ranging from the manual method to electronic methods have been proposed to address the various electoral malpractices associated with elections, however, the key issues of privacy, trust, and fairness in elections yet remain. In this research, we proposed an electronic voting system based on blockchain technology to address the identified issues of privacy, trust, and fairness. Smart contracts which kept track of votes in real-time and maintained the security of the electoral process were also proposed. The system was implemented on the Ethereum blockchain network, where Ganache was used to perform simulations of the voting process. We finally recommended that small-scale and medium-scale businesses could firstly adopt the system, after which, it could be implemented on a larger scale such as in national elections.

Index Terms— Ballot, Blockchain, Electronic Voting System, Ethereum, Real-time, Smart Contract, Vote.

1 INTRODUCTION

IN order to solve the problems associated with electoral malpractice in the form of duplicate votes, vote-buying, ballot snatching, ballot stuffing, results falsification, and encourage the increase in the confidence level of electoral output, there is a need for a system that captures the activities of the different phases in a typical electioneering process. The pertinent question then remains, how do we achieve a trusted voting system? This question wraps around voters' satisfaction. A quality voting system sure determines the quality of the leader. In a Nigerian setting, for example, the e-voting system has produced between 30% to 40% success in terms of providing electoral dividends and it is still yet to meet up with international standards [1]. This outcome is reflected in the quality of the electoral outputs and has thus been tagged flawed by foreign observers. This has led to a 10% decline in electoral participation culture in the Nigerian system from 1999 to 2007 [2].

Different e-voting technologies have been proposed in the literature such as Optical Character Recognition (OCR), tamper-proof balloting, and internet-based technology. Although these have been able to reduce the effect of electoral malpractice and increase the ease of voting by voters, they have not been able to fully guarantee a trusted system because of their easy to manipulate architecture. Many of these systems are easily bypassed by experienced riggers. This is made possible because of the centralized server architecture present in such systems, which gives room to the tampering of electoral results or a Denial-of-Service attack, leading to a disruption in the voting process due to the unavailability of the centralized server. Furthermore, these systems have shown an unsatisfactory level of transparency and accountability, because they provide an avenue to automate the voting process through an automated e-registration, validation, and voting process, only in a single repository that might not be readily available to the public for auditability purposes.

In this research work, we design and implement a framework for electronic voting systems based on blockchain technology to achieve trust, transparency, and timeliness of electoral results.

2 REVIEW OF RELATED WORKS

Ansari et al [3], developed a voter reconciliation system that involved a two-way process. Their research work focused on the voting process and post-voting process such that a reconciliation was later done to compare the electronic votes to the paper votes. Technically, this system was synonymous with having a double facet vote system but with some limitations to the system such as violation of voters' privacy and storage security.

Ayo, and Azeta [4], developed an integrated voice and Mobile Voting (m-voting) application to decrease admission barriers and ensure a rise in turnout of electorates during votes. Their research work eliminated the irregularities of manual paper voting while also enabling the visually impaired and physically challenged voters to participate in the election process. Later in 2010, Ayo, Daramola, Gabriel, and Sofoluwe [5] proposed an advancement of the project where an integrated all-in-one e-voting system that had the Electronic Voting Machine (EVM), Internet Voting (i-voting), and Mobile Voting (m-voting) was developed to ensure transparency, reliability, and convenience of voters. In a bid to address the multimodal identification and authentication, Ayo, Daramola, Gabriel, and Sofoluwe [5] developed a system that addressed the four major arm of electioneering in Nigeria, which are: the registration of voters, political parties and candidates, and the security of election data; voting (voter identification, authentication, and ballot casting); ballot tallying; and the transfer of votes from the polling booth to the various collation centers. This system provided an end-to-end electronic voting system to ensure adequate security.

Furthermore, the research work of Okwong [6], shows the prevalent situation of corruption in the electoral process that has militated against good governance in Nigeria. If Nigeria electoral situation is not known at all, there is one thing that rings a bell, which is the corruption that breeds throughout the election process, not necessarily by the electoral body but people in high position that have decided to break the rules of electoral processes to favor their selfish interest. Election fraud present in both pre-election and post-election phases includes ballot stuffing, ballot snatching, multiple registrations. The solution proposed by Okwong [6] provided an avenue to automate the voting process through an automated e-registration, validation, and voting process. This solution adopted the use of a single centralized database. The voters went through the registration phase after which they proceeded to the polling unit for validation. If properly registered, the system allowed the voters to vote and then set the voters' status to TRUE in the database.

Kuye, Coker, Ogundeinde, and Coker [2], proposed a system that was tailored to addressing voting anomalies by designing an electronic voting system for the whole election process that eliminated voting misconducts. This allowed the management, control, and monitoring of some of the activities of the regulatory bodies who were to register credible voters, electoral bodies, and contenders. The single centralized database of voters triggered the issue of unavailability in a situation of downtime on the system. The collation of results was done immediately after the voting in each polling unit was concluded. This helped curb the issue of ballot snatching, ballot stuffing, and vote rigging. However, there was no mechanism on secured transmission protocol to maintain the integrity and security of data.

The research work of Abayomi-Zannu, Odun-Ayo, and Barka [7] involved using Blockchain technology on m-voting to enable voters to effortlessly and conveniently cast their votes by making use of mobile devices. The system proposed a framework to safely keep votes and a multi-factor verification mechanism to verify eligible voters. A very similar work was done by Shukla, Thasmiya, Shashank, and Mamatha [8] where they developed an online voting application using Ethereum Blockchain technology which required the voters to have a high-end device to participate in the election process.

3 Methodology

3.1 Overview of Blockchain Technology

The client-server architecture is managed by a single entity having full access to the database with the ability to manipulate stored data in the database. A database administrator who is in charge of the data of an organization can decide to manipulate the records in the database for his or her selfish interest. For other use cases such as financial institutions with highly sensitive and confidential records, a single trusted entity is also usually responsible for the management of their organizational data. There is still a high probability that a hacker could infiltrate into their network and manipulate records in the database for their selfish interest. The best way to eradicate this prevailing problem is to take away the sole power from a single entity that can manipulate data. Blockchain ensures that this centralized power is distributed across the nodes within the network by the consensus mechanism present in the blockchain network. The data written on the blockchain network are known transactions, and once these transactions are written on the network they become immutable, hence ensuring data integrity and trust within the network.

Blockchain technology was adopted in this research work in the development of the electronic voting system due to its underlying security features and its fault tolerance. Below are some of the key characteristics of blockchain and how they, in turn, are useful to this research:

1. Cryptography: Blockchain provides an effective encryption mechanism that ensures the integrity of the transactions stored within the network. This can be seen in the hashing algorithm intrinsic to blockchain technology. The SHA-1, SHA-2, and SHA-256 are some of the common algorithms associated with the blockchain technology because of their unique hash function quality that creates unique outputs when given different inputs. Blockchain technology uses this hash function to make the transaction in the system immutable by producing a unique digital signature anytime anything is changed in a block. This is sometimes referred to as a fingerprint. Figure 1, shows the manipulation of the hash of a block, which is flagged as a tampered block.

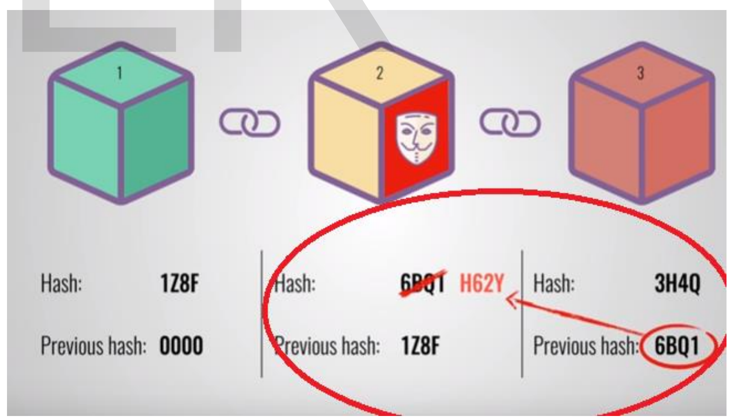

Figure 1: Tampered Block [9]

2. Immutability: Theoretically, it is possible for the system to be exploited by taking advantage of the 51% attack rule. This would require the hacker to control 51% of the nodes in order to produce a block that the remaining nodes would approve. This process is time-consuming and resource-intensive to be done by a hacker, and hence almost impractical to be performed.
3. Decentralization: The client-server architecture, as already established, requires a central repository of data and one or more entities responsible for the

maintenance of the information. This implies that the unavailability of the entity to manage the central repositories could lead to the downtime of the services relying on the data. Blockchain however ensures that no single entity has the sole power to control the entire network. All nodes jointly control the network, hence decentralization is ensured.

4. Anonymity: All transactions in a blockchain network are visible by all, but maintain the anonymity of the users making such transactions by recording their unique code called the public key on the blockchain, rather than displaying their personal information.

3.2 System Methodology

This research was premised on the idea of assigning voting rights to only eligible candidates and preventing electoral result manipulation. This delegated only a vote to a user and further ensured that vote counting was automated, fair, and transparent.

In this research, a vote was considered as a transaction that was added to the blockchain network to keep track of the tallied votes which were visible to all users in real-time. This ensured that there were no issues of manipulated records, that votes were verified, and no unlawful votes were added, further ensuring the transparency of the election process.

One smart contract was created per ballot. The smart contract creator, who was referred to as the chairperson, gave the right to vote to each address individually. The people behind the addresses could then choose to append their vote to a trusted candidate. At the end of the voting process, the *winningProposal* smart contract returned the largest number of votes.

The vote comprised two important parts, the voter's wallet address, and the choice he/she made, which was represented by the value TRUE and the value FALSE.

The system presented two attributes of the voter, which were the voter's name, and whether or not he/she had voted. A mapping named *votes* was used to store votes while the eligible voters' records were stored in a mapping called *votersRegister*. The *votes* mapping was declared as a private identifier so that voters could not read them directly. However, the *votersRegister* mapping was declared as a public identifier such that anyone could verify eligible voters.

A public variable *countResult* was created to store the total number of votes that were true. The variable was first initialized to 0. This *countResult* variable was used to keep real-time records of votes.

Another variable called *totalVoter* was created to keep records of the total voters in the *votersRegister*. This made it possible for the system to monitor in real-time, the total possible number of votes in the blockchain network as they changed, as opposed to tallying at the end of the voting process.

This whole process allowed only eligible voters to participate in the voting process. In addition, eligible voters could verify the authenticity of their vote by tracing their unique identifier on the register which was referred to as the transaction log on the user interface.

3.3 System Architecture

The architecture of the proposed system was a modification of the architecture of Abayomi-Zannu, Odun-Ayo, and Barka [7] as shown in Figure 2.

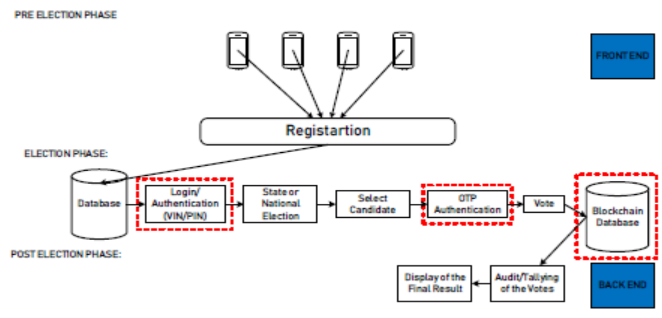

Figure 2: Architectural Framework of Abayomi-Zannu, Odun-Ayo, and Barka [7]

The architecture of this research in Figure 3 was a modified version of that of Abayomi-Zannu, Odun-Ayo, and Barka [7] due to its lack of real-time accessibility of electoral results and the inability of voters to verify their votes on the blockchain network. It is imperative that voters verify and identify their votes on the blockchain network with their unique transaction hash identifier generated at the point of voting to further give the voters the assurance that their votes counted.

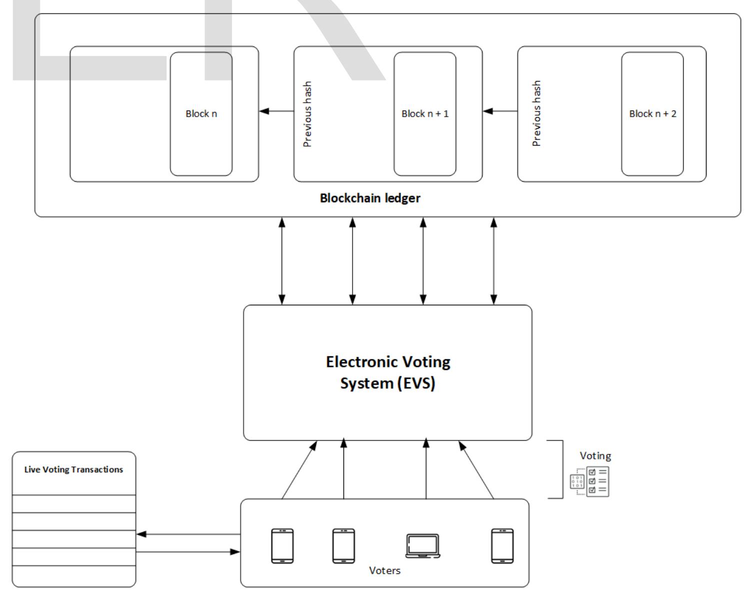

Figure 3: Architectural Framework of the Proposed E-Voting System

ISSN 2229-5518

4 System Implementation

The system implementation was divided into two phases which are:

1. Ganache Blockchain Deployment (Backend)
2. Electronic Voting System (Frontend)

4.1 Ganache Blockchain Deployment (Backend)

Ganache was installed at the backend of the application to interact with an Ethereum blockchain network. With the installation comes 10 free accounts preloaded with 100 Ethers (ETH) as shown in Figure 4. Each user has a unique address and a private key. Each account address will serve as a unique identifier for each voter in the election process.

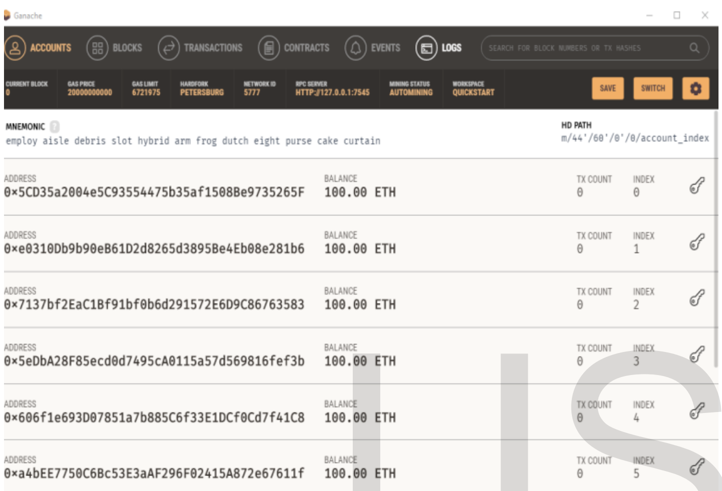

Figure 4: Blockchain users on the Ethereum blockchain network

The smart contracts were built and saved into a directory designated to store the smart contracts. All the business logic of the application resided in the smart contracts, which were in charge of modifying the Ethereum blockchain network. They allowed the registration and listing of candidates that participated in the election. They also kept track of all electoral results and their voters. All the rules of the election were governed by the smart contracts, by enforcing accounts to vote only once per election.

The system ensured that once a voter casts a vote, he or she is denied access to cast another vote, thus making the system resistant to a double vote count.

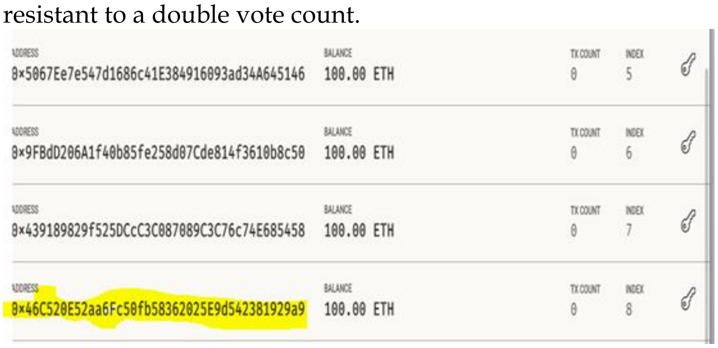

Figure 5: Index address

As shown in Figure 5, the highlighted address of index 8 in the Ganache network is used in the simulation network. The private key to the address was opened on the Ganache network to copy the address of the private key as shown in Figure 6. This address was then imported into MetaMask, the wallet system that interacts with the Ethereum blockchain, which was used to register the user for vote casting. Once in MetaMask, the user was then connected to the voting site where he or she was able to cast a vote for the preferred candidate.

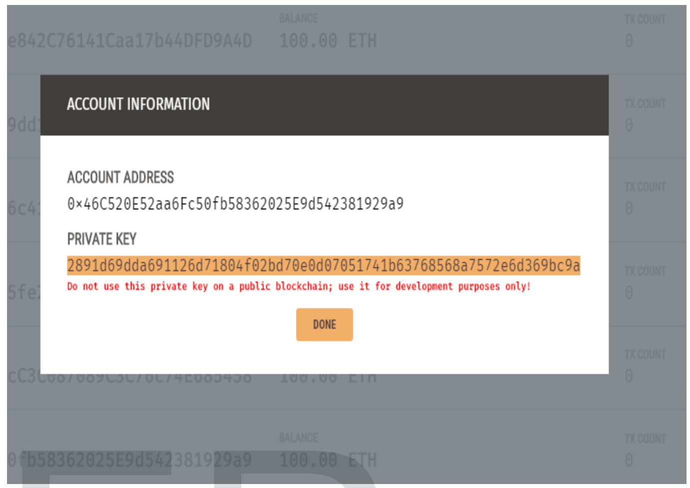

Figure 6: Private Key address

4.2 Electronic Voting System (Frontend)

A client-side application was designed using HTML, CSS, and JavaScript to communicate with the smart contract at the backend. The client-side application was designed so that it displayed a list of the candidates that were to be voted for and each user of the system was able to view the number of votes each candidate had received in real-time. As already established, the moment a vote was cast on the network by a user, the user lost the ability to cast another vote for the same election, and could only view the progress of the electoral results.

5 Results and Discussion

We now show snapshots of the system, illustrating the operation of the system.

1. Login and confirmation page: This allows eligible voters to confirm their identity on the Ethereum blockchain, after which they are assigned a unique ID to vote with as shown in Figures 8 & 9.

Figure 8: Confirmation page

Figure 9: Login page

2. Candidates Page: This shows a Graphical User Interface for the candidates to be voted for as shown in Figure 10.

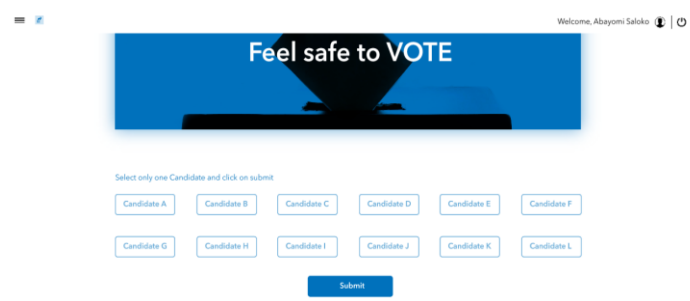

Figure 10: List of candidates

3. Voter's Account: This page shows the voters'ability to vote for a selected candidate. The page also shows the vote button for the voter to append his/her vote as shown in Figure 11.

Figure 11: Vote submit button

4. User View After Voting: This shows the hiding of the submit button from the voter after appending his or her vote for the chosen candidate as shown in Figure 12. This helps to avoid double votes. A unique transaction ID is generated for every vote transaction.

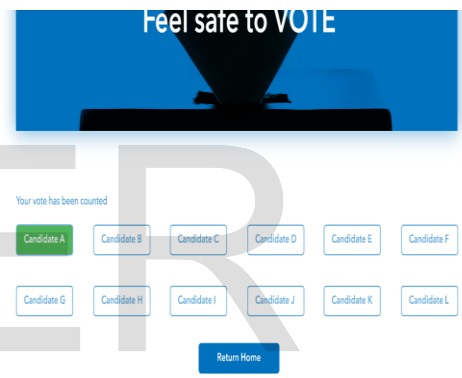

Figure 12 User view after casting vote

5. Real-time electoral result: This displays the electoral result in real-time with receipt of voter's transaction as hash ID as shown in Figure 13.

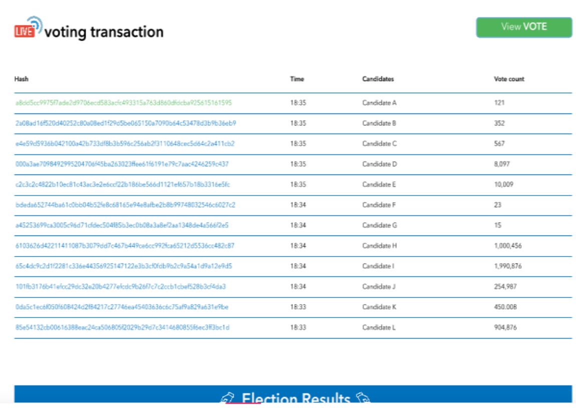

Figure 13: Real-time results

6 Conclusion

This research was aimed at ensuring the reduction in electoral malpractices that has led to non-transparency, unfairness, duplicate votes, and delayed electoral results. The above was achieved by using Ethereum blockchain technology, which is a distributed ledger spread across all nodes that are connected to the blockchain system or network. Blockchain technology ensures uptime because the storage and processing are not centralized. Blockchain technology has proven to be efficient in distributing immutable information across all nodes within the network, and thus, in this research, blockchain technology was used to ensure data integrity and further used to ensure transparency in the electoral process.

7 Recommendations

This research was proposed to curb the challenges plaguing voting systems, and more specifically the lack of real-time results and transparency. We recommend that all small-scale and medium-scale businesses adopt this Electronic Voting System based on blockchain to ensure fairness, privacy, and timeliness of electoral results thus encouraging transparency. Subsequently, it could be implemented on a large scale such as in national elections within countries, in order to ensure transparency in the electoral system.

References

[1] A. Shuaibu, A. Mohammed and A. Ume, “A Framework for the Adoption of Electronic Voting System in Nigeria,” *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 7, no 3, pp. 258-268, 2017.

[2] C. O. Kuye, J. O. Coker, I. A. Ogundeinde and C. A. Coker, “Design and Analysis of Electronic Voting System in Nigeria,” *International Archive of Applied Sciences and Technology,* vol. 4, no 2, pp. 15-20, 2013.

[3] N. Ansari, P. Sakarindr, E. Haghani, C. Zhang, A. K. Jain and Y. Q. Shi, “Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records,” *IEEE Security & Privacy,* vol. 6, no 3, pp. 30-39, 2008.

[4] C. Ayo and A. Azeta, “A Framework for Voice-Enabled m-Voting System: Nigeria a Case Study,” in *9th European Conference on e-Government*, London, 2009.

[5] C. Ayo, J. Daramola, O. Gabriel and A. Sofoluwe, “An End-to-End e-Election System Based on Multimodal Identification and Authentication.,” in *6th International Conference on e-Government*, Cape Town, 2010.

[6] A. E. Okwong, “IT-Based Solutions to the Electoral System in Nigeria,” *West African Journal of Industrial and Academic Research,* vol. 5, no 1, pp. 127-139, 2012.

[7] T. P. Abayomi-Zannu, I. A. Odun-Ayo and T. F. Barka, “A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication,” in *International Conference on Engineering for Sustainable World*, 2019.

[8] S. Shukla, A. N. Thasmiya, D. O. Shashank and H. R. Mamatha, “Online Voting Application Using Ethereum Blockchain,” in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018.

[9] X. Decuyper, “How does a blockchain work,” [Online]. Available: https://savjee.be/videos/simply-explained/how-does-a-blockchain-work/. [Acessed 2021].