Australian Journal of Science and Technology

ISSN Number (2208-6404)
Volume 6; Issue 4; December 2022

Original Article

# A framework for a hybridized online and offline voting mechanism based on blockchain technology

**Oladipupo Ridwan Olayinka[1], Ajayi Olusola Olajide[2], Adedeji Adebayo Clinton[1]**

[1]Proprein Labs, Ibadan, Oyo, Nigeria, [2]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Ondo, Nigeria

**ABSTRACT**

Voting is one of the most important ways to ensure fair representation and equal voice when making decisions. The larger implications for each decision, the more people who participate in the process. As such, it can become difficult to accurately and efficiently keep track of each voter's eligibility and legitimacy to participate. Technology has positive impacts on many aspects of our social life. In this light, the internet has been a fertile ground for innovation and creativity. Among such disruptive innovations are blockchain and USSD technologies. Voting security has been a heavily debated topic amongst all kinds of people. From political to technological perspectives, keeping our elections secure, accessible and transparent would be the best way to curb election violence such as killings, thuggery, ballot snatching, manipulations, vote buying, and issues such as inconclusive elections, card reader error among others in our sustainable world. As such, blockchain technology has the ability to introduce a system that is seemingly impossible to hack to the table, combined with the isolated ease of access, interactive communication, and security provided by the USSD technology. The customizable menu-driven mobile-based protocol (USSD) is available on every GSM-enabled mobile device. In this paper, we propose a hybridized online and offline voting mechanism, that is based on a transparent ballot box (blockchain). The objective of combining the two schemes would be to achieve a decentralized architecture to run and support a voting scheme that is transparent, reliable, secure, efficient, accurate, credible, accessible, interactive, responsive, independently verifiable, free, and fair election process.

**Keywords:** Availability, blockchain, confidentiality, election, e-voting, integrity, offline voting, privacy, security, USSD

Submitted: 07-08-2022, Accepted: 22-08-2022, Published: 30-12-2022

## INTRODUCTION

Online voting - or e-voting (electronic voting) - allows participants to cast their vote using information and communications technologies which includes the internet, SMS, or other digital services. Electronic voting is often seen as a tool for making the electoral process more efficient and for increasing trust in its management. Voting through the internet is just one form of electronic voting (e-voting). In general, speaking, e-voting refers to both the electronic means of casting a vote and electronic means of tabulating votes. Using this definition, many voting methods currently in use in the United States already qualify. Other methods include Punch-card voting system, Optical scan voting system, and Direct-recording electronic (DRE) voting system. Properly implemented e-voting solutions can increase the security of the ballot, speed up the processing of results and make voting easier. However, the challenges are considerable. If not carefully planned and designed, e-voting can undermine the confidence in the whole electoral process.

According to Osho *et al*.,[1] E-voting is seen as the ability of a nation to improve her electoral process. Non-electronic voting systems are often replete with many flaws, including high cost and easy manipulation. Paper ballots, direct counting, and other manual electoral processes have proved unreliable due to rigging, misplacement of ballot papers, over-counting or undercounting of votes, mixing up votes and changing of ballot papers and results. Electronic voting in polling stations is in place in some of the world's largest democracies, and

**Address for correspondence:** Oladipupo Ridwan Olayinka, Software Development and Solution Delivery, Proprein Labs Technologies, Nigeria. E-mail: oladipuporidwanolayinka@gmail.com

internet voting is used in some, initially mainly small and historically conflict-free, countries. Many countries are currently considering introducing e-voting systems with the aim of improving various aspects of the electoral process. E-voting is often seen as a tool for advancing democracy, building trust in electoral management, adding credibility to election results and increasing the overall efficiency of the electoral process. The technology is evolving fast and election managers, observers, international organizations, vendors and standardization bodies are continuously updating their methodologies and approaches.

An e-voting system must be accessible to every eligible voter and provide a high level of security. However, this system has been found to be vulnerable to various security challenges and threats, including stored central data leakage/disclosure, selling of votes, and the presence of certain malware on voter's machine, to mention but a few.[2] Although there are strong encryption schemes applicable to address issues concerning confidentiality, integrity, and authenticity, there is a need for further technological implementations to address issues of availability, which consequently enhances overall security.[3] Essentially, electronic voting requires a level of security higher than the other components, including e-commerce.[4]

However, properly implemented, e-voting solutions can eliminate certain common avenues of fraud, speed up the processing of results, increase accessibility and make voting more convenient for citizens - in some cases, when used over a series of electoral events, possibly even reducing the cost of elections or referendums in the long term. Unfortunately, not all e-voting projects succeed in delivering on such high promises. The current e-voting technology is not problem-free. Legislative and technical challenges have arisen in some cases; in others, there has been skepticism about or opposition to the introduction of new voting technologies. The inherent challenges of e-voting are considerable and linked to the complexities of electronic systems and procedures. Many e-voting solutions lack transparency for voters and even for election administrators. Most e-voting solutions are only fully understood by a small number of experts and the integrity of the electoral process relies largely on a small group of system operators instead of thousands of poll workers. If not carefully planned and designed, the introduction of e-voting can undermine confidence in the whole electoral process. It is therefore important to devote adequate time and resources to considering its introduction and looking at previous experiences of electronic voting.

In the first use of blockchain technology in a U.S. federal election, the State of West Virginia used Voatz's mobile voting application to enable overseas voters to vote in the 2018 U.S. midterm elections. A total of 144 voters from 31 countries participated in the pilot. The Voatz application relies on blockchain technology to create an immutable record of the votes cast. It also uses cybersecurity software to detect malware on smartphones, and biometrics for identification and authentication. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes has their own copy of the distributed ledger that contains the full history of all transactions the network has processed. There is no single authority that controls the network. If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and, moreover, it could have the potential to make e-voting more acceptable and reliable.[5]

However, the intention behind this research work is to design a framework for a hybridized online and offline voting mechanism based on blockchain technology that is accessible, secure, efficient, effective, with low cost, reliable, transparent, verifiable, free, and fair. The framework is designed to achieve the following; voting registration process will be made available online on the system. In essence, the voter's registration would be exceedingly fast and more accurate, speed up voter's authentication, preserve voter's secrecy, and make the storage, counting and transmission of votes 100% secure, thereby making voting and electoral process a priority to the citizens and government; Implement an offline voting mechanism that would only allow valid voters to cast their vote once through the USSD protocol available on every GSM-enabled mobile device. Restriction would be set, such that any subsequent attempt or tamper would be disregarded; Provision for auditing and certification would be made available, allowing stakeholders access to procedures and documentation; Training, professional development, and civic and voter education would be ensured. Well-informed stakeholders will find it easier to trust the system.

Several researchers have proposed the use of various cryptographic schemes most especially encryption algorithms (both symmetric and asymmetric) to solve problems around security on e-voting system, yet the system has been found to be vulnerable to various security challenges and threats, including stored central data leakage/disclosure, selling of votes, and the presence of certain malware on voter's machine, to mention but a few.

However, if not carefully planned and designed, the introduction of e-voting can undermine confidence in the whole electoral process. It is therefore important to devote adequate time and resources to considering its introduction and looking at previous experiences of electronic voting. Hence, the need for a hybridized online and offline mechanism based on blockchain technology.

In this work, some existing works on e-voting systems are reviewed. The basis for evaluating the performance of the systems is the level of ubiquity - capacity to provide equality of access- privacy and security support.

In the development of any system, e-voting systems inclusive, certain requirements must be considered as primary objectives, since having a perfect system is almost infeasible. One common requirement is security. Most voting data and process security are based on encryption schemes through public key infrastructure, and certificates, for example, in Zissis,[4] Ray and Narasimhamurthim,[6] Diehl and Weddeling,[7] Olaniyi *et al*.[8]

In 2013, George and Sebastian[9] proposed a secure and efficient frontend voting protocol using a trusted platform module for remote internet voting with trusted third-party authentication protocol. The protocols provide true, trustworthy authentication of the involved parties and remote machine using a trusted platform module. The attestation by the TTP for authenticating the remote platform keeps its anonymity. The anonymity of the voter is maintained by performing the validation and tallying of the vote cast by separate Validator and Tallier. The Validator validates the vote without knowing the vote content and the Tallier tallies the vote without knowing the voter identity. In essence, only the validated vote will be forwarded to the Tallier. Hence, voters verify that his/her vote is counted in the final tally. The proposed system is vulnerable to many attacks varying from generic internet attacks to system specific attacks, as the voting is done on the internet from a remote platform. There are many methods to defend against generic internet attacks. This paper concentrates only on the analysis of system specific attacks.

In 2013, Alaguvel and Gnanavel[10] proposed an Offline and Online E-Voting System with Embedded Security for Real Time Application. The authors in their research make use of the facial recognition mechanism, Finger vein recognition algorithm, Iris matching detection and One Time Password for the voter's authentication and authorization. However, they were able to ensure a secure system to some extent, but the ease of use and privacy were not achieved.

In 2016, Osho *et al*.[1] proposed a hybrid electronic voting system that combines the capabilities of the DRE and online electronic voting system, offering a platform for online and offline voting. The system is designed to support voting through direct-recording, online poll-site, and remote e-voting systems. However, for online voting, the system is implemented as a cloud application. Voting is done online either remotely through a PC connected to the internet, or at an e-voting polling kiosk. For eligible voters who reside or intend to cast their vote in locations where internet is inaccessible, the DRE, administered at a polling kiosk, is implemented with a computer with a keyboard or touch screen to cast their votes, with vote tally stored on the computer memory storage, after which the results are synchronized with the cloud. The design also provides an audit system for logging every process. The authors only focused on two elements of information security - integrity and availability. Confidentiality was not ensured, and system evaluation was not carried out.

In 2017, Yifan[11] proposed an e-voting system based on blockchain and signature. In their research, the generated protocol satisfied the properties of ballot-privacy, individual verifiability, eligibility, completeness, uniqueness, robustness, and coercion-resistance. However, it does not fulfill the needs of fairness and receipt-freeness. In the performance evaluation, the protocol works efficiently for ring signature, especially when the number of the voter is less than 3000. Therefore, the efficiency of the ring signature algorithm is limited by the number of participants.

In 2018, Wei and Wen[12] proposed a blockchain-based electronic voting protocol that makes use of blockchain technology properties to enhance its security features. The system can secure the identity of every voter and ensure that all the vote results recorded are tamper-proof. It provides advantageous properties for e-voting systems such as authenticity, integrity, verifiability, anonymity, availability, and a general consensus from every participant. The system does not rely on human trust but on computational cryptographic trust. However, this method does not foster the accessibility of voters remotely.

In 2019, Kumar *et al*.[13] presented a proof of concept system for developing an e-Voting system that utilized the Ethereum blockchain. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it (as discussed under Security Analysis). Issues like "booth-hijacking" are well tackled in the proposed solution as the user does not need to visit a booth to cast his vote. Moreover, the system is completely transparent and the blockchain stores the logs of each of the transactions in a very secure manner which provides the assurance to the voter that his vote has been successfully casted and he may verify the same later at any point of time.

## MATERIALS AND METHODS

### Methodology

This study adopts the use of hybridized USSD protocol (that combines web, SMS, USSD, and/or IVR.) and blockchain technology. USSD is one of the channels enabling technology to reach almost anyone. The technology has been used in emerging markets for more than a decade and is sometimes considered to be the "ancestor" of mobile apps. This comes

with the benefit of enabling market users to have access to their internet-based services without the need for internet-enabled phones. For instance, several mobile operators offer their user's access to Facebook through USSD. Using this service, users can view their news feed and update or like a status without having to connect to the internet and all at very little cost. However, with blockchain, we can secure a platform that lets users cast their votes with an unprecedented degree of trust and transparency.

In the pursuit of a successful implementation of this work, the following procedure shall be followed, as illustrated in Figure 1:

### *Information gathering*

Extensive and adequate information will be gathered in the field of this study. Some of these include extensive literature review of past research works in this domain of study. Also, experts will be consulted and information extracted on how the process is being carried out and the needed caution to take into consideration in the design of the system. The information gathering approach that will be used in this stage is the online survey (using Google form) where information will be mined through the online poles (Twitter, LinkedIn, Instagram, Facebook, etc.). These procedures, parameters, and the information obtained will be used in building the proposed system.

### *Modeling*

Modeling involves graphical methods and nontechnical language that represent the system at various stages of development. The universal modeling language (UML) will be used to model the development and the implementation of this research work. Various UML Diagrams such as the Use Case Diagram, System Flow Diagram and the Sequence diagram will be deployed to show the various interactions and relationships that exist between objects, entities in the system. The Use Case Diagram is used to illustrate a unit of functionality provided by the system. The main purpose of the use case diagram is to help visualize the functional requirements of a system, including the relationship of actors (human beings who will interact with the system) to essential processes, as well as the relationships among different use cases. The actors include the electoral candidates, voters, and the administrator while the system is the e-voting system. The use case describes how the user interacts with the system such as the voters register for election, vote the electoral candidates, have access to election updates, and audit the system. While the System Flow Diagram shows the flow of interaction of the actors with the system.

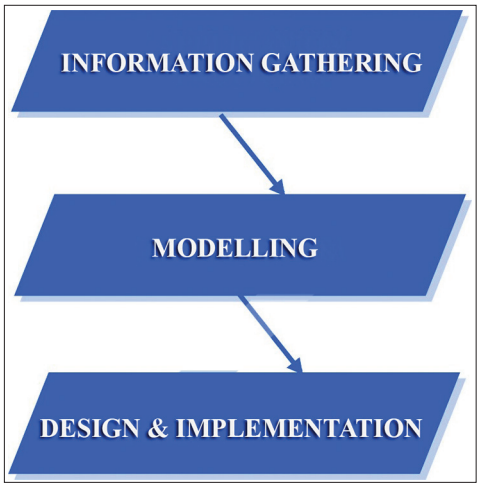


**Figure 1:** Diagram showing the research methodology

### *Design and implementation*

At this stage, the research work which was modeled in the previous stage will be designed and implemented. It will be implemented using hybridized USSD protocol on distributed decentralized servers (blockchain). The online portal will be designed with Figma as a prototyping tool, React framework for frontend development, and Python/Django on blockchain for backend development.

## Model

A model can come in many shapes, sizes, and styles. It is important to emphasize that a model is not the real world but merely a human construct to help us better understand real world systems. The model illustrated in Figure 2 below is deployed as a guide to successful implementation of this research work.

The model consists of the following components,

i. Online Portal
ii. Validation Server

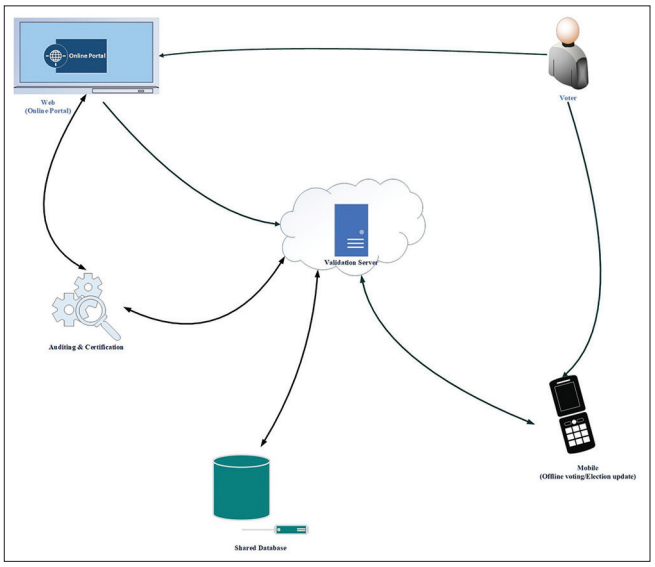


**Figure 2:** Architectural model for the study

iii. Offline voting system
iv. Audit and Certification
v. Shared Database

### *Online portal*

The citizens are allowed to register for the election online and provide the necessary credentials such as birth certificate, state of origin etc. The system would however determine the eligibility of the individual after validation. Voting is enabled on the mobile phone (offline) through the USSD protocol, the results of the election and the statistics will be available and accessible online through the portal.

### *Validation server*

It contains the registration details of all eligible voters. Hence, a voter must be validated on this server before he/she can be granted permission to vote offline.

### *Offline voting system*

This is a stand-alone component of the entire e-voting system, the USSD allows users to have access to their internet-based services without the need for internet-enabled phones. Users typically dial a short code on their phone, for example, *177#, and get access to a menu where they can be accredited, vote for the candidate of their choice, and subscribe for election updates.

### *Audit and certification*

This is an audit service that provides for auditing of the entire process with certification. These are important confidence-building measures and should be transparent, allowing stakeholders access to procedures and documentation.

### *Shared database*

All the votes are stored on blockchain. The information stored on the ledger is protected by a form of cryptography that provides each user with two types of "keys" - one key is kept private, and the others are made public - which work together like the two-key system used to access a safety deposit box. The private key, similar to a password or PIN, gives a user the ability to "lock" or "unlock" their information and control when, and by whom, it is accessed. Other trusted "nodes" on the network can then be given a public key so that they can read the unlocked information and double-check that it actually comes from the user.

## EXPECTED RESULT AND DISCUSSION

A system is considered secure if it fulfills all the five elements of information security -confidentiality, integrity and availability, authenticity, and non-repudiation. In this study, we compare the performance of the existing systems based on the level of ubiquity, capacity to provide equality of access, privacy, and security. George and Sebastian[9] worked on integrity and authenticity,[10] worked on authenticity, Osho[1] worked on integrity and availability, and Yifan,[11] Wei and Wen[12] worked on confidentiality, integrity, authenticity, and non-repudiation.

However, our study addresses all the five elements. The Government and the entire citizens as the stakeholders will benefit from the system. Such that, it would make positive change in the fate of the nation, influence participation and activism in politics. The government is potentially able to increase voter's turnout, reduce costs, increase voter's confidence, renew interest in the political system, and ensure the most democratic process possible. The system would ensure faster results, build trust, put an end to gratification of electoral officers by political parties thereby manipulating election results.

It helps save life and thereby encourages more participation of people of every race to be involved in not just the decision making of the government but in the electoral system of the country. Voters gain a better voting experience at the comfort of their home with no apathy. Voters are more confident that their vote will be correctly counted without manipulation, and are able to vote more easily and efficiently. The system would stop voters from common election faults, such as picking too many or no candidates, ballot box hijacking, thereby increasing the general effectiveness of voting. The system would provide the ease of voting for citizens who are otherwise geographically isolated from election centers. The system would also reduce fraud, by eliminating the opportunity for ballot tampering. The system increases accessibility i.e. It is easier for the disabled (physically challenged) to vote independently.

## CONCLUSION

It is widely known that the benefits of the electronic system of voting as against the use of traditional voting methods cannot be overemphasized. This study, in its own view, has contributed to existing knowledge primarily by presenting a seamless system with an architectural framework that guarantees transparency, reliability, efficiency, accuracy, credibility, responsive, accessibility, independently verifiable to virtually all categories of voters to be enfranchised, and supports security of voting data and processes.

The architecture of the system presented inherently supports security of voting data, by separating and assigning duties to different servers, with accessibility, by means of well-established protocol, and privacy among other features. However, this assertion was not evaluated. Hence, this area is open for further studies. This study has focused on the three elements of information security - confidentiality, integrity, availability, authenticity, and non-repudiation.

## REFERENCES


1. Osho LO, Abdullahi MB, Osho O. Framework for an e-voting system applicable in developing economies. Int J Inf Eng Electron Bus 2016;6:9-21.
2. Chaeikar S, Jafari M, Taherdoost H, Chaeikar N. Definitions and criteria of CIA security triangle in electronic voting system. Int J Adv Comput Sci Inf Technol 2012;1:14-23.
3. Zissis D, Lekkas D. Securing e-government and e-voting with an open cloud computing architecture. Gov Inf Q 2011;28:239-51.
4. Zissis D. Methodologies and Technologies for Designing Secure Electronic Voting Information Systems. (Unpublished PhD Thesis). Greece: University of the Aegean; 2011.
5. Hardwick FS, Gioulis A, Akram RN, MarkantonakisK. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; 2018.
6. Ray I, Narasimhamurthi N. An anonymous electronic voting protocol for voting over the internet. In: Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems. San Juan, CA: IEEE; 2001. p. 188-90.
7. Diehl K, Weddeling S. Online Voting Project-New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles. Electronic Voting; 2006. p. 213-22.
8. Olaniyi OM, Arulogun OT, Omidiora EO. Design of secure electronic voting system using multifactor authentication and cryptographic hash functions. Int J Comput Inf Technol 2013;2:1122-30.
9. George V, Sebastian MP. Remote internet voting: Developing a secure and efficient frontend. CSIT 2013;1:231-41.
10. Alaguvel R, Gnanavel G. Offline and online e-voting system with embedded security for real time application. Int J Eng Res 2013;2:76-82.
11. Yifan W. An E-Voting System Based on Blockchain and Signature. United Kingdom: School of Computer Science, University of Birmingham; 2017.
12. Wei CC, Wen CC. Blockchain-based electronic voting protocol. Int J Inf Visualiz 2018;2:4-2.
13. Kumar S, Darshini N, Saxena S, Hemavathi P. Voteeth: An e-voting system using blockchain. Int Res J Comput Sci 2019;6:11-8.