ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

Harnessing Benefits of 4th Industrial Revolution Technology: The Need for Blockchain-Based Electronic Voting System in Nigeria

Oladimeji Biodun S. (PhD), Madu Fortunatus U., Oyedepo Victoria A., & Eze Chimdiyya (PhD)

Lecturer, Department of Computer Science, Federal Polytechnic Nekede, Owerri Imo State.
Senior Lecturer, Department of Computer Science, Federal Polytechnic Nekede, Owerri Imo State.
Principal Lecturer, Department of Computer Science, Federal Polytechnic Nekede, Owerri Imo State.
Lecturer, Department of Computer Science, Federal College of Education (Technical) Omoku Rivers State, Nigeria.

ABSTRACT: Blockchain is a distributed ledger technology that allows digital assets to be transacted in a peer-to-peer decentralized network. Those transactions are verified and registered by every node of the network, thus creating a transparent and immutable sequence of registered events whose veracity is provided by a consensus protocol. E-voting system is an electronic way of casting and counting votes. It is an efficient and cost effective way for conducting a voting process in real time. However, globally, concerns on security networking and privacy of communication for e-voting have evolved. Securing e-voting is very urgent and has becoming a popular topic in the area of communications and networking. In Nigeria, citizens have complained over the integrity of national electoral umpire simply because Nigeria is still using traditional voting system. Integrity is put to test on every of our election result especially by the opposition parties. Electronic voting systems are one example of a use case that can be improved by the block-chain technology. We therefore, try to apply block-chain technology to our electoral process in order to improve the security of e-voting in Nigeria. This paper proposed block-chain based electronic voting in order to have safe, free, fair, and transparent elections in Nigeria. Finally, we recommend this system to be absorbed by Independent National Electoral Commission for reliable, effective and efficient electoral system.

KEYWORDS: E-voting, Blockchain, Peer to Peer, INEC, Network etc.

I. INTRODUCTION

Today in our country Nigeria considerable numbers of citizens do not trust their government especially when it comes to political activities like elections [1]. This makes the election a very important event in our modern democracy. The problem with the existing ballot system is that it can be easily manipulated by power hungry organizations [2]. Democratic countries have been experiencing dictatorial regimes which have introduced widespread terror among their people. People have had their human rights violated and their fundamental freedoms provided by their constitution taken away. In such an environment, having a fair and transparent election is something that is paramount for the freedom most people enjoy today. The pitfalls of the current system of ballot voting are being taken advantage of by people or organizations looking to gain power. In the African countries of Uganda, Kenya and Nigeria there has been widespread controversy over their elections in recent years. The election of 1946 in Romania was heavily rigged. The communists took over Romania and abolished the multi-party system to gain complete control of the country [2]. Furthermore, Opposition parties in Nigeria still believe 2019 general elections were massively rigged in farvour of the ruling party APC. These instances of controversial elections could all have been avoided if the counting process was free, fair, transparent and verifiable. The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an election umpire like INEC or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral flaws such as voter fraud, ballot stuffing and booth capturing. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization which put its

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

integrity to test. The proposed system solves most of the issues mentioned above and can be implemented in Nigeria and other countries in globally.

Our proposed system looks to eliminate the aspect of trust from an election to make it more free, fair, secure and transparent. The system uses existing technology such as a client server architecture integrated with a blockchain system to ensure aspects such as transparency, security and traceability are achieved without sacrificing privacy for voters. We believe the cost of building the system will be substantially less as compared to the cost of running a ballot based system. There are substantial social benefits to using the e-voting system. Also the system will usher in easier and quicker voting process which will lead to higher voter turnout. Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its general elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An E-Voting system suppose to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

Blockchain technology is a distributed ledger technology that allows digital assets to be transacted in a peer-to-peer decentralized network. Those transactions are verified and registered by every node of the network, thus creating a transparent and immutable sequence of registered events whose veracity is provided by a consensus protocol. By enabling smart contracts to be deployed into a blockchain platform, the number of possible use cases for this technology improves considerably thereby eliminating the need for third parties and, therefore, allowing many processes, in both the public and the private sectors, to become more efficient and economical. E-voting systems are one example of a use case that can be improved by the blockchain technology. In this paper, we highlight and discuss how blockchain technology can solve major electronic voting systems challenges facing Nigeria as a country. Additionally, the components and functionalities of our proposed blockchain-based electronic voting system are presented and briefly explained [7].

In today's world, widespread mistrust towards the government and interference in countries' processes by external actors have made the democratic process of voting more critical than ever. Democratic countries have been experiencing dictatorial regimes which have introduced widespread terror among their people. People have had their human rights violated and their fundamental freedoms provided by their constitution taken away. In such an atmosphere, having a fair and transparent election is something that is paramount for the freedom most people enjoy today. The pitfalls of the current system of ballot voting are being taken advantage of by people or organizations looking to gain power. In the African countries of Uganda and Kenya there has been widespread controversy over their elections in recent years. The election of 1946 in Romania was heavily rigged. The communists took over Romania and abolished the multi-party system to gain complete control of the country [2]. These instances of controversial elections could all have been avoided if the counting process was fair, transparent and verifiable. The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an Election commission or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral scams such as voter fraud, ballot stuffing and booth capturing [3]. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization. The system that is being proposed solves most of the issues mentioned above and can be implemented in Nigeria and other countries globally.

II. BACKGROUND OF THE STUDY

Elections in Nigeria are a critical part of her budding democratic process, however, just like most aspects of Nigeria's democracy, the electioneering process are still being blurred by specs of debris from several years of colonial rules followed by the military influence spanning about three decades and a dose of an aggressive political elite unwilling to relinquish her hold to what has become a lucrative business for most. The history of elections in Nigerian state has been characterized by threats to statehood based on the manipulation of ethnicity as a divisive mechanism for the acquisition of political power by political actors; the fragile nature of political cum democratic institutions is acquainted with poor democratic culture among Nigerian citizen.

Every four years, the elections serve as an unusual common ground for the elite and the over 87.8 million Nigerians living in extreme poverty and that is the common ground for both ends. There seems to be a painstaking effort by both

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

ends of the divide to maintain the status quo, efforts by the political elite to keep the average Nigerian disinterested in the issues of governance, election inclusive [16]. Elections in Nigeria from 1999 to date have continued to recycle in vicious violence and unimaginable manipulation especially from the political elites; this has attracted the attention of the local and international community [15]. The violence coupled with the glaring disorganized manual election process has discouraged a sizeable number of citizens from participating in the electoral process. Many citizens' faith in the integrity of the electoral process has also waned over the previous years due to the incessant stories of rigging. The number of registered voters is always significantly more than the actual votes cast and these numbers have significantly dwindled in the past years. Experts suggest most electorates are unwilling to participate in the elections primarily because of the conventional practice that requires voters to stand in queues for long hours as witnessed by less than 50% voter turnout in 2015 presidential election in Nigeria [15].

The Independent National Electoral Commission (INEC) has bemoaned the insufficient representation of women in political positions in spite of the good percentage of women in the voting population of Nigeria. Women occupy about 5.8% of the political offices in Nigeria while men occupy about 94.2% of the political offices. "Global statistics for gender parity indicates that in 2015, out of 188 countries, Nigeria was 152nd in the Human Development Index in Gender Inequality and 118th out of 192 countries in 2017″ [16]. It is worthy to note that in Nigerian women are still being marginalized due to the style of leadership inherent in the country. Despite the challenges women are facing, it was discovered that women activism and advocacy, education of women, positivity on the part of successive governments towards women empowerment and interest of women to participate in politics is getting a lot of positive energy.

2019 Election

The total number of registered voters for the 2019 election is 84,004,084. This is an increase of 15.3m from the total number of voters registered in 2015. Though Nigeria Population is put at roughly 200 million according to National Bureau of Statistics in 2019, only 84,004,084 registered while others were either afraid of coming out to vote for fear of election related violence or some are underage [15].

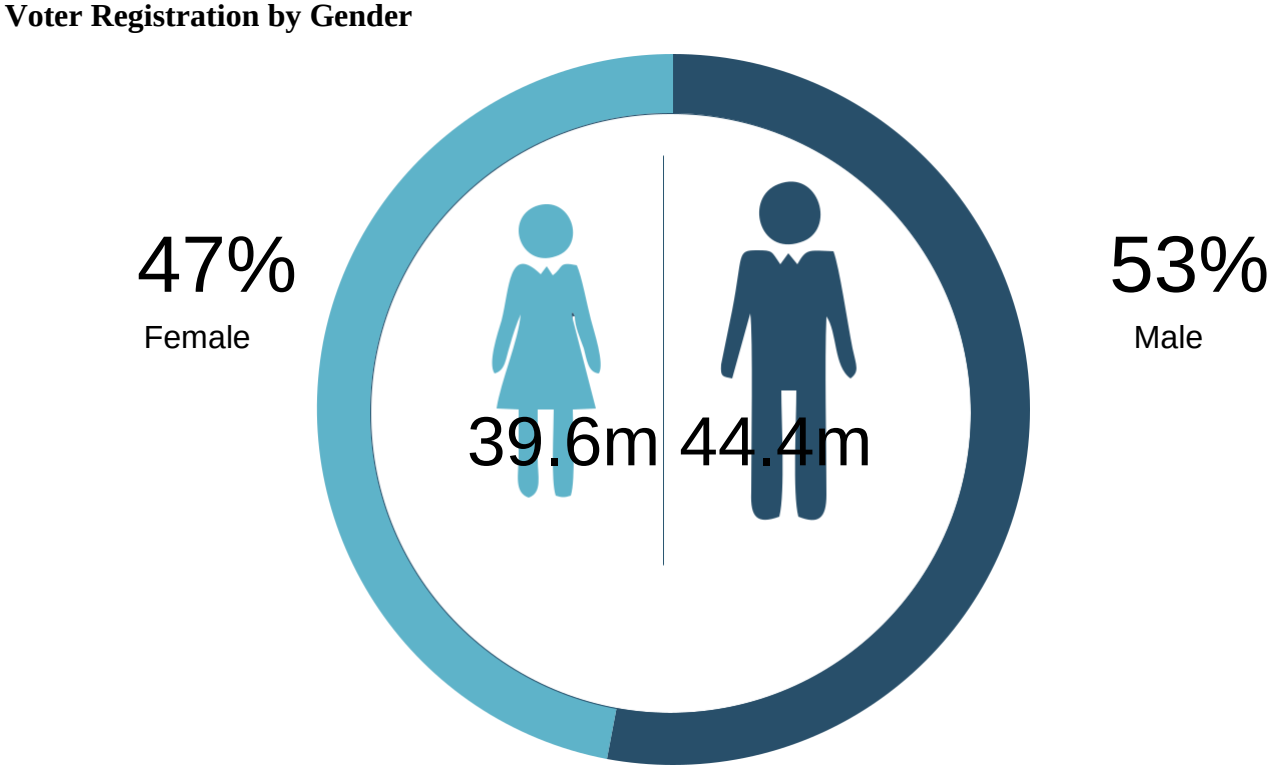

Figure1.0: Voter Registration by Gender (courtesy: inec.com)

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

III. SIGNIFICANCE OF THE SYSTEM

This system is very significant if Nigeria want to have free, fair, transparent and hitch-free elections. Security of life and properties of the citizens should be considered utmost; Nigerians have witnessed countless number of killings related to electoral exercises. There are a lot of flaws associated with the existing ballot system. Traditional elections satisfy neither citizens nor political authorities in recent years [15]. They are not fully secure since it is easy to attack votes. Also it threatens privacy and transparency of voters and the integrity of INEC have been questionable over time. Additionally, it takes too much time to count the votes and it exposes the electorates to unnecessary dangers. So if our election system is designed to exploit blockchain technology, it will go a long way in reducing frauds at all levels and perhaps restores the lost glory of our electoral system.

IV. LITERATURE SURVEY

On January 10, 2016, an organization called the APLA was formed using blockchain recording technology as a cornerstone to protect and exploit the democratic functioning of governments such as the United Arab Emirates, India, Russia and the West Indies. Netherlands or organizations in Dubai. These application environments operate in a gradual framework for admission to information, interfaces, and grand contracts [13].

In Argentina, there is an association called Democracy Red and Democracy OS. It is free and open-source online software that is used for democratic purposes. There are three levels: Collect political questions, talk about these topics, and decide on an explicit proposal. The goal of this task is to create a democratic stage for every city or government. In addition, Mexico has taken this step to gather criticism of people under the Open Source Information Agreement, and an association in Tunisia called I Watch used this open-source tool to give people a more fundamental voice when they do vote [11].

In India, the company is trying to exploit the obstacles in its business. Andhra Pradesh has for some time been the first block-block technology state to register its records, computer-aided identity, cross-border payments and transportation as test companies. These use cases for pigs depend on conceptual evidence. They also send a group to numerous conferences or workshops to understand the technology and its implications for their business. And also, to face a number of challenges in using blockages, vendor/phase, onboard partners, development environment, security issues, and Cohesion problems [9].

In Boston, USA UU., January 8, 2018, a blond company and an IBM person named Voatz who use blocking technology to make transparent, efficient and secure agreements. In addition, they focused on four key regions to achieve success, such as Versatile security, voter darkness, unsurpassed nature and clarity through a secure mobile phone, multi-source identification assurance process, and biometric data Motivation and assurance are based on Blockchain. In this context, the declaration of identity takes twenty to four hours and strengthens one million votes per second. It is also used in government, organization and university elections in private or open elections [10][11].

In the New York Times, Washington Post, there were shortcomings in 2016 in the presidential race. In the US elections of November 2018, Voatz was therefore used as a portable application of her choice to cast unreliable votes and use blocking technology on a permanent basis [11]. In Australia, Horizon State has a defence system based on blocking technology. Of course, there are plenty of locations for your items: a secure structure, a warning of problems, voters can access the material to the crusher, and investigative tools tell you about the viability of individual fights and how did the voters behave. In December 2017, Russia had a program called Active Citizens Program. This program uses a private phase of Ethereum to improve voting and strengthen trust between the voter and its legislator. In addition, 1000 transactions per minute will be settled if the entire democratic voting result is recorded in the registers and all the centres that can see the result [9]. The Indonesian government used a portal as a portable application of their choice on the island of Sumatra in July, which was created by the Australian organization Horizon State. They want to grow as a nation beyond their wealth [10].

Blockchain

Blockchain was first introduced by Satoshi Nakamoto (a pseudonym) [10], who proposed a peer- to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution [11]. Blockchain is secure by design, and an example of a system with a high byzantine failure tolerance [12]. Bitcoin is considered the first application of the Blockchain concept to create a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

blocks of transactions. Each block in the chain is linked to the previous block in the chain. The first block in the chain is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain.

IV. METHODOLOGY

In this research, secondary sources of data were employed. The researchers consulted online publications, periodicals, National Bureau of Statistics (NBS), Independent National Electoral Commission (INEC), Budgit etc. From our collective deductions we were able to summarize that elections related political unrest, if not eradicated, would be drastically reduced.

Proposed System

The proposed system involves a client server architecture integrated with a block chain system. The minimum requirements needed by a voter are a smart-phone or a computer with a webcam and an internet connection. If these are not met alternate arrangements such as pop-up cyber cafes and computers at public buildings must provide access to disadvantaged voters. This would be sponsored by the Federal Government of Nigeria so to remove that burden off the electorates.

System Requirements

The e-Voting system will include four main requirements that can be illustrated as shown below:

Authentication: Only people already registered to vote can cast a vote. Our system will not support a registration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure manner. Therefore, the system should be able to verify voters' identities against a previously verified database, and then let them vote only once.

Anonymity: The e-Voting system should not allow any links between voters' identities and ballots. The voter has to remain anonymous during and after the election.

Accuracy: Votes must be accurate; every vote should be counted, and can't be changed, duplicated or removed.

Verifiability: The system should be verifiable to make sure all votes are counted correctly. Beside the main requirement, our solution supports mobility, flexibility, and efficiency. However, we will limit this paper's discussion to the four main requirements.

The Blockchain Model

The first transaction added to the block will be a special transaction that represents the candidate. When this transaction is created it will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate. Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election [9]. Every time a person votes the transaction gets will be recorded and the Blockchain will be updated.

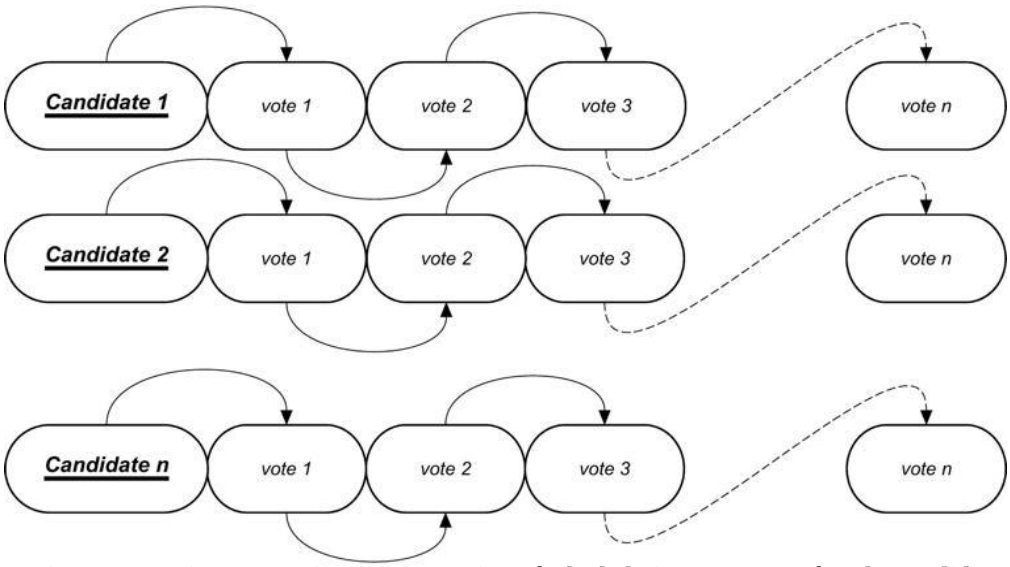

Figure 2.0: Diagrammatic Representation of Blockchain Structure of each Candidate [4]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other. The Blockchain is decentralized and cannot be corrupted; no single point of failure exists [4]. The Blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the Blockchain. The voting system will have a node in each district to ensure the system is decentralized.

System Prototype

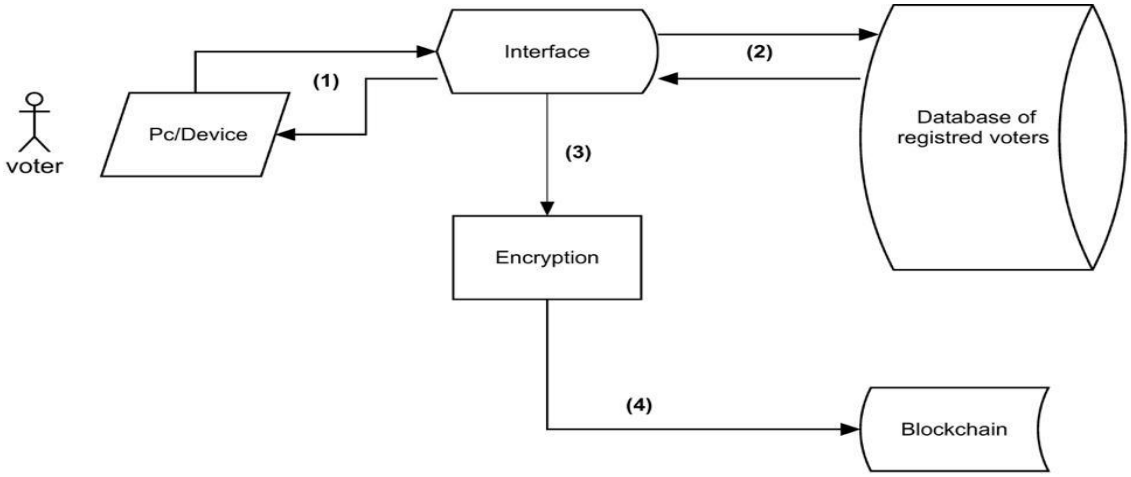

Figure 3.0: Prototype of the Proposed System

Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-Voting system will use his Social Security Number his address, and the voting confirmation numbers provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack [8], where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface.

Encrypting votes: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA-256, which is a one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match [8]. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved.

Adding the vote to the Blockchain: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding Blockchain. Each block gets linked to the previously cast vote.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

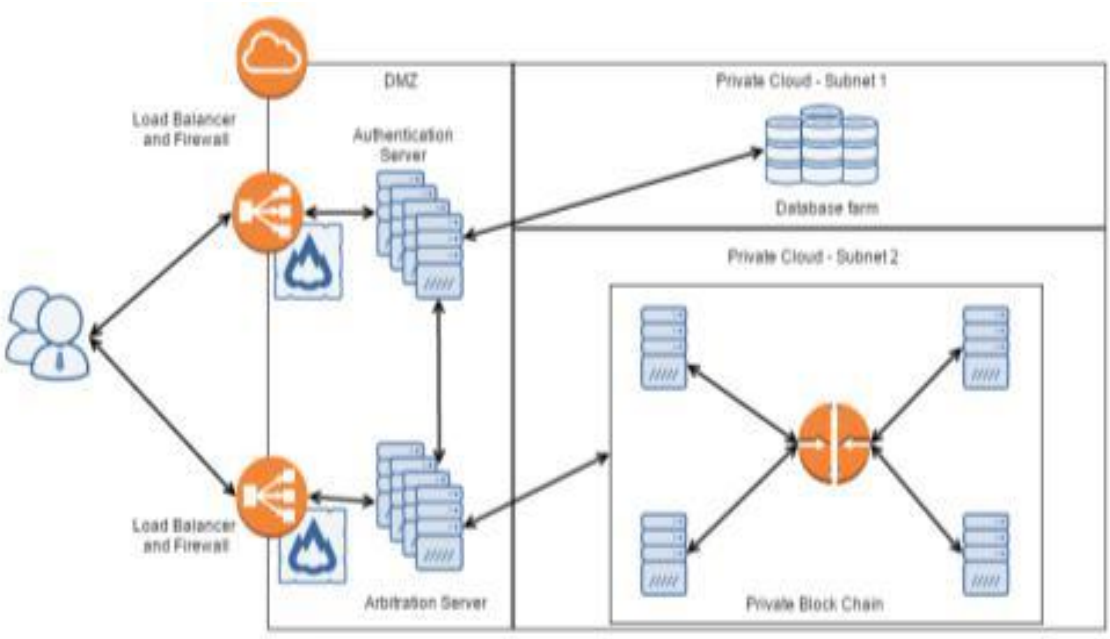

Figure 4.0: Network Architecture of the proposed System [7]

The above diagram shows how the user interacts with the different parts of the system. The system will be explained in two parts–explaining the functionality of each part and the processes associated with the system.

Proposed System Components

There are four main components to the system as explained below:

User

The user must have a smart-phone, laptop or any device with a browser and a front facing camera. The user must also have an internet connection to register and vote as well. If the user does not have a computer or an internet connection, he/she could go to a public building such as a library or a school which does have computers to register to vote [14]. These could be kept open all day during voting registration and voting days to ensure people with low sources of income do not get left out.

Authentication Server (AS)

The Authentication Server is a traditional centralized web server. It has a backend database connected to it which has the information of all the citizens in the country. This system is used by people to register to vote for their elections. People create login accounts when they register. It also creates accounts on the blockchain system for the users when they vote. The blockchain account is used by the Arbitration Server to vote for a candidate of the users' choice. The AS also authenticates the token provided to the Authorization Server by the user while voting [14].

Arbitration Server (AR)

The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The AR is a blockchain thin client that sends the users' vote to a blockchain node [3]. It also sends the user the key to encrypt their vote. The AR sends the users' vote to the appropriate node to be added to the blockchain. The user can verify their vote using the AR as an intermediary.

Blockchain system

The blockchain system is the system on which the actual voting takes place. The users' vote is sent to the one of the nodes on the system depending on the load on each node. The node then adds the transaction to the blockchain depending on the smart contracts that exist on each node. The smart contracts are the rules that the nodes follow to not only verify but also add the vote in the system. Each node follows the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly [6]. The system will currently have node server in each state to ensure distributed network traffic on the system.

Processes in the system

The process of voting has two steps in the old process, i.e. registering to vote and the process of voting itself. The proposed system will have an extra step, i.e. the ability for the user to verify their vote. This is an important step where

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

the user can get a confirmation of their vote. The other steps include counting the votes by the organizer and recounting in case of any discrepancies [11].

Registration

The process of registering to vote begins with the user interacting with the Authentication Server via a website. The AS contains information about voters in a database. The user enters his/her Personally Identifiable Information (PII) and scans supporting documentation to upload into the system along with an email address. The users' picture is also taken for verification. If the information is verified and is correct, the user is allowed to create an account. The user enters a username of their choice and a password to log in. This information is stored separately and not linked to the users' PII [10]. This ensures privacy and anonymity while voting. Also an entry is made next to the users' database entry storing whether he/she has registered to vote. If the users' information cannot be verified, he/she is not allowed to create an account. All the information between the user and the AS is sent using TLS v1.2 protocol to ensure it is all secure.

Voting

The process of voting is a multi-step process. It involves verifying your identity with the AS and then voting using the AR. On the day of voting each candidate is given an account on the blockchain system so they can get votes. There is also a "Abstain account" for abstained votes to be sent to. During voting day, the user logs in to the authentication server using the username and password created in the previous step. An image of the user is taken to ensure that the user is the owner of the account. This image is compared with the image taken during registration [14]. A small video of the user is taken before they log in and is sent to the Authentication Server. Using the Affectiva API the AS can identify user emotions based on machine learning technology [4]. If the system detects fear, the users' session is stopped and told to retry after 5 minutes. While logging in for the second time if the system detects fear again, the user must go to their local polling center such as a library to vote. This system would reduce the impact of the issue related to voting under duress. Once the user logs in, their system would create a public key which they would send to the Authentication Server. The AS would add associate the key with the username. The key would be used to create an account for the user on the blockchain system to vote. A specific amount of ether (currency the user can use to vote) is added to the users' account which enables them to vote. The AS would then send a session token back to the user. The user would be redirected to the AR. The user would provide the AR with the session token, would verify it with AS. The verification and generation of token between the AR, user and AS is done using the Modified Needham-Schroeder protocol. This protects the system from impersonation and man in the middle attacks [12][13].

The AR would send a verification message to the user along with the public key of the blockchain node to which his/her vote would be sent. The user would encrypt their vote with the public key and send it to AR. This would ensure that the AR cannot read the users' vote and hence the vote would remain a secret. The AR would send the encrypted vote to the appropriate node. The node would decrypt the message with their private key and send a specific amount of ether from the users' account to the candidates' (or to the Abstain account if they would like to forfeit their vote) blockchain account [19]. Each node would verify the transaction according to the smart contracts. These contracts would verify a particular transaction was a duplicate one or no and check its validity. After this process the node would pass this transaction to other nodes in the blockchain system.

Vote Verification

The process of verifying the vote depends on the type of election it is. Some elections allow for interim results and some do not. In either case the voter must get a confirmation that his/her transaction has been approved by the blockchain system. In case of the election that allows interim results, one of the nodes of the blockchain could be made publicly accessible. It would have a website similar to https://blockchain.info_where a user could enter their public key to verify whether their vote was counted. This node would not have the ability to add any transactions to the system. This will be implemented through smart contracts. It will only be a reader of the transactions. This will reduce the attack surface of the system. If the organizers of an election want to keep the interim results a secret, he/she could only get a binary verification via the AR. Since the AR is a thin client it would act as an intermediary to verify the transaction [3]. At the end of the election in above case, the user will be able to check the result for the election.

Vote Counting

The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice [12]. The candidate with the highest amount of ether in their account wins the election. For users who abstained from voting, their ether will be sent to an Abstain Account. This ensures their vote does not get misused.

Recounting the cotes

There are instances of disputes in the results of an election. These can be resolved in the proposed system easily. The entire tree associated with a single account root can be made public for people to verify if their vote has been tallied or not [5]. This makes the system transparent for users. Since no one knows which user is associated with which account,

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

it protects the users' anonymity in voting. The public keys for each transaction in the blockchain system can be mapped to accounts in the AS. The list of public keys generated gives the list of people who voted. By mapping this list with the public keys associated with each transaction, the election can be verified [8].

V. CONCUSSES IN THE BLOC KCHAIN

With decentralized systems and especially with our e-Voting Blockchain-based system, a problem of concusses may occur. This happens when different voters cast t heir votes at approximately the same time. As explained earlier in this paper, when a voter casts a vote, it will be linked to the previous vote to create a chain that neither corruptible nor changeable. In the case of concusses, our solution is to use the Longest Chain Rule, which is used by Bitcoin to resolve the same problem [9]. Let us suppose all blocks in the system are synchronized and they are at block 100 1. Three new votes have just been cast at the same time and they were all assigned the number 1002 in the chain. We will call these three new blocks 1001-A, 1001-B, and 1001-C.

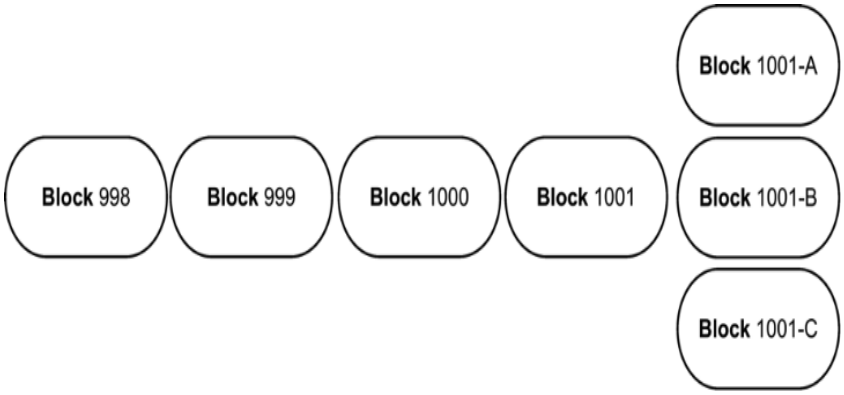

Figure 5.0: Concusses in the Blockchain [5]

Let us assume Block 1001-A is introduced first to the Blockchain, and so the system will add it to the chain as the successor of Block 1001. Later on, Block 1001-B is introduced to the chain [5]. The system will hold on to it and wait until another block arrives. If Block 1002-A is introduced to the system, the Blockchain will assume that Block 1001-A is the valid block and will keep building on the longer chain. Block 1001- B and 1001-C will be considered orphans blocks.

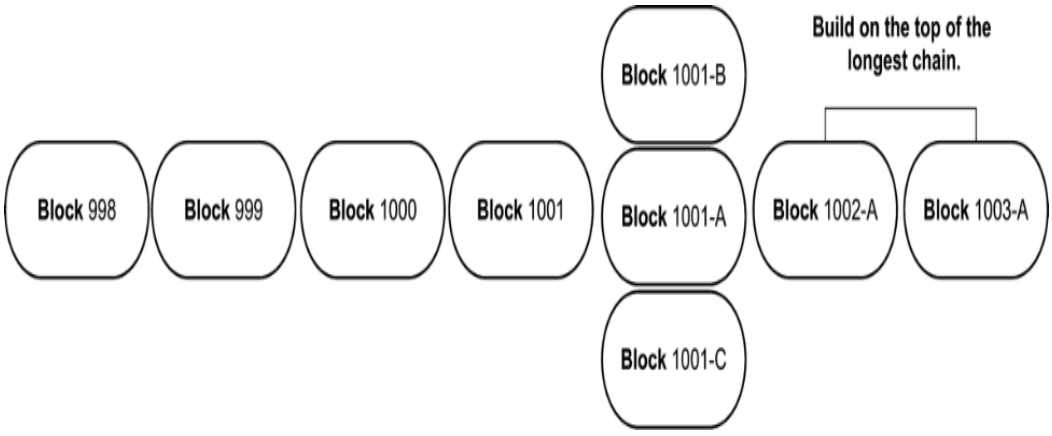

Figure 6.0: Longest Chain Rule [5]

Because we have a different chain for each candidate, orphan blocks will no longer be a problem since they contain the same information (vote) as the other blocks, and they will be considered when votes are counted.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

VI. ANALYSIS

In this system, the whole voting information is hold at the highest leveled blockchain. So voting information of the whole country can be reachable instantly at any time after it is synchronized. It will not be a problem to explain results of the election, and lots of time that is being spent in order to count votes will be saved. This will change the old and ineffective system and bring a modern and effective system to Nigeria. This will also save lots of energy dissipated on election activities as well as saving human and material resources. According to calculated statistics considering the data taken from official statistics site of NBS [11], it is known that there were about 85 million voters at the 2019 general elections in Nigeria. Considering this number, it is assumed that 800 clusters (clusters include voting centers under them) would be enough. This is not a random number; it is chosen according to population of the country and bottleneck probabilities at the levels. Environmental change is a big factor here, due to the latency. As applicable to all systems, there is a potential threat for the proposed election system. As Yli-Huumo et al. [8] states, if any attacker can get 51% of the computation power of the whole network then it can manipulate the data and this is called 51% attack [8]. In the proposed system, node can only be gathered via hacking or stealing the voting machines. However, stealing 51% of the voting machines of the country is nearly impossible because in the elections law enforcements are protecting the voting centers therefore any physical theft can be identified and prevented [8]. Apart from the previously mentioned risks, in case of a disaster citizen who had to vote on the voting machine that has damaged or unavailable to server can be distributed to the nearest voting centers with legal inspections of the supreme committee of elections (INEC). Citizens who vote on the voting center that has any problem due to technical problems and disasters can cast their votes in different voting center. Although disaster can damage the voting machine, blockchain keeps secure all the casted votes. Therefore even in extreme cases during the election day, elections can be completed safely without any doubt.

VII. DRAWBACK

In using this system, we believe that voters will use a secure electronic device to cast their vote. Even while our system is secure, hackers have the ability to cast or alter a vote using malicious software already installed on the voter's device. One of the limitations of this system is its inability to change a vote in case of a user mistake. The user is allowed to cast his vote only once. Finally, we recommend that subsequent researchers work on the identified lapses.

VIII. CONCLUSION

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. Existing paper based elections system do not provide integrity and trustworthiness. In this journal, we proposed a blockchain based e-voting system that will provide free, fair, transparent, secure and fast voting system for Nigeria elections. Although, our system is suitable to apply even in another country, however integration could be hard work. This is because each country operates different systems of governance. In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. By using blockchain technology in the development of an electronic voting solution we expect to enhance the security of those solutions and provide a transparent and auditable electronic voting platform. With the project coming to its end, it is already possible to conclude that blockchain has the potential to improve electronic voting systems by inherently solving their major limitations and issues. While our developed electronic voting solution remains only a functional prototype, the trials it was subjected to allow us to conclude about the viability of the use of blockchain technology in the development of this kind of systems. In the future, we intend to test our blockchain-based e-voting system in real conditions in order to evaluate its performance under heavy loads.

REFERENCES

[1] M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Proceedings of Computer Science, vol. 141, pp. 239-246, 2018.
[2] P. Tarasov and H. Tewari, "The Future of E-voting," IADIS International Journal on Computer Science and Information Systems, vol. 12, no. 2, pp. 148-165.
[3] Bartolucci, S., Bernat, P., & Joseph, D. (2018). SHARVOT: Secret SHARe-Based VOTing on the Blockchain. 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 30-34.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

[4] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, vol. 88, pp. 173-190, 2018.
[5] B. Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain", Procedia Computer Science, vol. 129, pp. 234-237, 2018.
[6] Internet: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake [Nov. 25, 2018]
[7] Alharby, Maher, and Aad van Moorsel. "Blockchain Based Smart Contracts : A Systematic Mapping Study." Computer Science & Information Technology (CS & IT), 2017
[8] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLOS ONE, vol. 11, no. 10, 2016.
[9] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6.
[10] R. Krimmer, A. Ehringfeld, and M. Traxl, "The Use of E-Voting in the Austrian Federation of Students Elections 2009," Internet:https://pdfs.semanticscholar.org/6b8f/34a5bd3e7eabc7e3a9a3f008187 e4415e26a.pdf [Nov. 26, 2018]
[11] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.
[12] S. Ølnes, J. Ubacht and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Government Information Quarterly, vol. 34, no. 3, pp. 355-364, 2017.
[13] A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology," Available:https://www.economist.com/sites/default/files/plymouth.pdf [Nov. 20,2018]
[14] A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology," Available: https://www.economist.com/sites/default/files/plymouth.pdf [Nov. 20,2018
[15] Independent National Electoral Commission (INEC) available via https:www.inec.com/2019electionsreport. Accessed on 10th December, 2019.
[16] National Bureau of Statistics (NBS) available via https:www.nigerianstat.gov.ng. Accessed on 14th December, 2019.