**Optimization of Nigeria Electoral Process using Blockchain Technology.**

**Ishola Eniola O. andSamaila G. Zainab**

**Kings Embedded Solutions Limited.**

**Abstract**

*This paper proposes Blockchain technology-based solution to build an open, trusted and decentralized system for the Nigeria Electoral System focusing on the public key cryptography, privacy, and verification steps for Nigeria Electoral Process. The Blockchain-based electoral system technology was developed from a set of state transition rules to a method for creating blocks for all contesting parties in Nigeria, to mechanisms for checking the voter’s accreditations, validity of election, and the full chain election monitoring systems. In the later part of the paper, we discussed the “design experiment” for the proposed Blockchain application for the Nigeria Electoral System will be a success, making the entire voting processes way faster, reduced paper-works, and more secured voting system. The success proves the use of a distributed ledgers to run the voting processes will prevent fraud & identify theft.*

**Keyword:** Blockchain, Security, Cryptography, Public key, Privacy & Distributed Ledger.

**INTRODUCTION**

Nigeria want to hold its elections and prevent voters’ fraud and eliminate vote rigging. Immutable publicly – viewable ledgers or recorded votes for the Independent National Electoral Commission (INEC) would make elections more democratic and fair. To accomplish this without a trusted party, elections must be publicly announced using the public ledger in order to enable cryptography with integrity.

First and foremost, what is a blockchain?

“A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography” (Wikipedia, 2018). The concept of blockchain initially came from Stuart Haber and W. Scott Stornetta in a 1991 paper called “how to time stamp a digital document”. Most of the ideas and concept of blockchain are actually present in that paper.

Blockchain is a public electronic ledger – similar to a relational database - that can be openly shared among disparate users and that creates an unchangeable record of their transactions, each one time-stamped and linked to the previous one. “Each digital record or transaction in the thread is called a block and it allows either an open or controlled set of users to participate in the electronic ledger. Each block is linked to a specific participant” (Lucas Mearian, 2018).

Blockchain is a foundational technology, with the potential to create new foundation for our economic and social systems. “Blockchain has been heralded as a foundational technology which will transform every single business in the decade. It’s unlikely to be a wholly disruptive technology that attacks traditional business models with a lower-cost solution that overtakes other networking technology quickly” (Karim Lakhani, 2018). A Blockchain is a sequence of blocks of data in which each block, other than the first, is cryptographically linked to its predecessor. “A Blockchain network is a peer-to-peer network in which peers collaborate to achieve a common goal by using a Blockchain” (Ephraim Feig, 2018). “A decentralized network uses distributed ledger technology for the efficient and secure transfer of business assists between member” (Mark Parzygnat and Don Thibeau, 2018). “The distributed ledger technology, better known as Blockchain, has the potential to eliminate huge amounts of record-keeping, save money and disrupt IT in ways not seen since the internet arrived” (Lucas Mearian, 2018). As a result, the model involves a great deal of trust, as all the participants in the network must reach a consensus to accept transactions.

Figure 1. How blocks are linked cryptographically © SuperDataScience

Most important of all, it’s secure. The database can only be extended; previous records cannot be changed—or, at least, there’s a very high cost if someone wants to alter previous records. “Blockchain can only be updated by consensus between participants in the system, and when new data is entered, it can never be erased. The Blockchain contains a true and verifiable record of each and every transaction ever made in the system” (Lucas Mearian, 2018).

Fig. 2. More concepts to blockchain ©SuperDataScience

However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley’s capitalists, listed the Blockchain ​ distributed consensus model​ as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin’s Blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond (Michael Crosby & Nachiappan et al, 2015).

**Types of networks**

© 42TEK, Inc. 2017

Fig. 3. Types of Network.

**PROBLEMS STATEMENTS**

1. To eliminate Changeable Records of Votes
2. To eliminate Double Voting/Alteration of Votes
3. To eliminate Identity Theft
4. To eliminate Election Manipulation/Vote Rigging
5. To upgrade the existing Central Authority Systems with state INEC collation centers to a Distributed Authority Systems.
6. There is a need for a distributed consensus where each and every political parties, party candidates and voters, past and present, involving captured data/votes can be verified at any time in the future.
7. There are challenges with the existing electoral system limit the numbers of voters due to its inflexibility which doesn’t create equal opportunities for all individuals that might take a shift from their initial registered state (voters location) to another state (new location) at the time of the election permanently.

**RELATED WORK**

The current digital economy is based on the reliance of a certain trusted authority. Our all online transactions rely on trusting someone to tell us the truth - it can be an email service provider telling us that our mail has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third party sources can be hacked, manipulated or compromised beyond (Michael Crosby & Nachiappan et al, 2015).

This is where the Blockchain Technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus ​where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus ​and anonymity ​are two important characteristics of Blockchain technology beyond (Michael Crosby & Nachiappan et al, 2015).

There are a variety of Blockchain permutations, and they fall mainly into one of the two categories – public or private. Public Blockchain allows anyone to see or send transactions as long as they are part of the consensus process. There are also consortium Blockchain, where only a pre-selected number of nodes are authorized to use the ledger. Private Blockchain, in contrast, restrict the ability to write to a distributed ledger to one organization (Lucas Mearian, 2018).

Electoral processes of various sorts have also benefited from the deployment and the use of Blockchain technologies. Follow My Vote is a startup using distributed ledgers to run voting processes and prevent fraud and identity theft. One of the potential advantages is that voters using Blockchain can verify their voting choices using their private keys at any point in time.

Ukraine is one country that has jumped into this area. The country will use E-vox, an Ethereum-based distributed ledger for local elections. Implementation has already started in a couple of towns.

The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of Blockchain technology involves “​ smart contracts​”. Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met, then the parties involved in a contractual agreement can automatically make payments as per the contract in a transparent manner (Lucas Mearian, 2018).

Blockchain technology is finding applications in wide range of areas—both ​ financial​ and non-financial​ (Michael Crosby & Nachiappan et al, 2015).

Financial​ institutions and banks no longer see Blockchain technology as threat to traditional business models. The world’s biggest banks are in fact looking for opportunities in this area by doing research on innovative Blockchain applications. In a recent interview Rain Lohmus of Estonia’s LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications.

Non-Financial​ applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the Blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved.

Fig. 4. Blockchain Used Cases ©Fujitsu

**PURPOSE/FINDINGS**

1. The proposed solution uses the Blockchain and IOT technology to build an open, trusted, decentralized and tamper-proof system, which provides the indisputable mechanism to verify that the data of voters has existed at a specific time in the network.
2. Kings Embedded Solutions uses distributed ledgers to run voting processes and prevent fraud & identify theft. One of the potential advantages is that voters using Blockchain can verify their voting choices using their voters card number at any point in time.
3. It saves operational cost, reduced paper works and voting time.
4. The blockchain-based solution is instantaneous and immutable.
5. To harness the Nigeria Electoral Process with the power of Blockchain using hash validation.
6. To build a decentralize, distributed ledgers, Blockchain-based electoral system.
7. Blockchain is predicted to become like TCP/IP and PKI – the technologies we use every day when we use the Internet (David Snyder, 2017)
8. Hundreds of companies are experimenting with Blockchain to enhance the overall business process and securities.

Blockchain can be utilized in many different fields as a solution to the problems that a standard database might have. One such problem can be seen in voting. Recently, it was revealed that a major U.S. voting machine manufacturer had installed remote access software on some systems. This software allowed for the alteration of votes when counting the total. Instances like this create a lack of trust in America's voting system, as seen in a recent poll: "Exclusive poll: Majority expects foreign meddling in midterms". This poll suggests that only about a quarter of Americans feel confident that their vote is being counted. Blockchain would solve this issue by providing a distributed ledger that would ensure your vote is counted since the ledger you own is the same as the one counting the total (Linux FoundationX, 2018).

**ORIGINALITY/VALUE**:

To the best of my knowledge, this is the first work that proposes for the integration of Blockchain and IOT technology into the Electoral System in Nigeria.

**PAPER TYPE:** Conceptual Paper

**CONTRIBUTION OF PAPER**

This paper aimed to optimize the existing Nigeria Electoral System to a blockchain-based Electoral System which was achieved using a set of state transition rules to a method for creating blocks for all contesting parties in Nigeria. A framework was developed and employed at the conceptual stage, before the development of the blockchain-based solution, electoral system basically on sets of rules that provides the basics that ask for specifics relating to the structure of the blockchain network dynamics to be implemented. The optimized blockchain-based electoral system provides a mechanism for checking the voter’s accreditations, validity of election, and the full chain election monitoring systems which was achieved by modeling, model analysis and architecture designs on the blockchain technology interpreted into the election system.

1. **Understanding SHA-256 Hash.**

A cryptographic hash (sometimes called ‘digest’) is a kind of ‘signature’ for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text (Chris Veness, 2017). The algorithm behind SHA256 Hash was developed by NSA. SHA256 Hash is very secured and a lot of application in the whole world use it to store passwords, documents, and in fact in blockchain is used as one of the core things, core principals building blocks of blockchain.

A hash is not ‘encryption’ – it cannot be decrypted back to the original text (it is a ‘one-way’ cryptographic function, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare ‘hashed’ versions of texts, as opposed to decrypting the text to obtain the original version.

Fig 5. SHA256 Hash ©SuperDataScience

Such applications include hash tables, integrity verification, challenge handshake authentication, digital signatures, etc.

* ‘challenge handshake authentication’ (or ‘challenge hash authentication’) avoids transmitting passwords in ‘clear’ – a client can send the hash of a password over the internet for validation by a server without risk of the original password being intercepted.
* anti-tamper – link a hash of a message to the original, and the recipient can re-hash the message and compare it to the supplied hash: if they match, the message is unchanged; this can also be used to confirm no data-loss in transmission.
* digital signatures are rather more involved, but in essence, you can sign the hash of a document by encrypting it with your private key, producing a digital signature for the document. Anyone else can then check that you authenticated the text by decrypting the signature with your public key to obtain the original hash again, and comparing it with their hash of the text.

Using the SHA256 Hash, it will always reproduce the same hash if we put in the same data. That is logical because like a human, if we take the same person and check for his finger print and take the same person and check for his finger print it will always be the same finger print without change.

In the figure shown below, blocks and hashes, we can see the demonstration hash generated for the given data below.

**Data:** “Nigeria Blockchain-based Electoral System”

**Hash:** “7b94d0bc8f7cdc960d2fd228c335bf9657316d1d0f24a9a26281d68091ff70e5”

Fig. 6a. SHA256 (Hash & Block). ©SuperDataScience

Another thing is that, if we change one time the “system” to “systems”, it will completely and entirely change the whole hash. See the Fig 6b below.

**Data:** “Nigeria Blockchain-based Electoral Systems”

**Hash:** “3b8d6a716989e0c83b77f6b40b515816436e4b0c916fa37577ba305d66e32b83”

The total Hash character generated is “**64 bits”** and 64 raised to the power of 4 is 256; **64^4 = 256.**

Fig. 6b. SHA256 (Hash & Block) ©SuperDataScience

**The 5 requirements for the Hash Algorithms.**

There is certain requirement for it be useful;

1. It has to be **One-Way**. You cannot go from the hash to the data. In case of a finger print, you can only use the finger print to get the Hash, you cannot use the Hash to get the finger print.
2. It has to be **Deterministic**. Meaning that, if I take the exactly the same document and run to apply the Hash algorithm again, I will get exactly the same result.
3. It has to be **Fast Computation**. We will see why it is truly important in the entire blockchain development process.
4. The **Avalanche Effect**. It is an ultra-high requirement of the Hash algorithm. The Avalanche Effect means, if we take the same document and make a tiny little change of data in the document, then the Hash will be absolutely different. It is called the Avalanche Effect because the way it is been implemented in the algorithm.
5. It **Must** withstand collisions. Sometimes, one in 60million (1 – 60,000,000) we may have same people with same result, same finger print. And same goes with the Hash algorithm the amount of digital data that we have, is much greater than the number of variations of the 64 character of the Hash algorithm and representation. Hash algorithm has to be able to withstand artificial collision that for instance pirate can create which is the problem because if a pirate can create an artificial collision of the document to access the Hash algorithm then they will forge the document.
6. **Immutable Ledger**

An immutable ledger simply means a record that cannot be changed. If a pirate tries to alter any information in the block, its hash will change, thereby affecting the next block and so on.

Fig 7. Immutable Ledger ©SuperDataScience

The longer thee chain becomes the more practical impossible to change the ledger because one changes made will affect the entire blocks because they are cryptographically linked together.

1. **Distributed Peer to Peer (P2P) Networks**

In a distributed P2P network, we have numbers of computers, and these computers are connected together on the network. A P2P Network is a very important part of how blockchain technology works, and why it’s so solid and secure. It could be thousands of computers, millions of computers to keep all records of transactions. Everything will be connected by means of cryptography keys.

Fig 8. A new block is added to computer 1 ©SuperDataScience

A ledger of public transactions (votes) distributed across peers of network. Once a new block is added that information’s is communicated throughout the network and that block is added further to other network until all the computers are have these blocks though it might take some time.

Fig 9. Information communicated and that block was further added to all the network ©SuperDataScience

As more transactions are added to the blockchain. And now someone tries to hack one of the entry and take away some data stored on a network, and once they do, other blockchains on that particular network are attacked because they are cryptographically linked together as shown in the figure below.

Fig 10. A blockchain network under attack ©SuperDataScience

Now since the peers are constantly checking to see if the blockchain does not match with the blockchain in the network, quickly the peers will signal to the computer to let it know the blockchain has been under attack/hacked, and it will check the majority since they are in consensus with the it has, that means, it will understand that it has been hacked, what will happen is that, it checks the value that is different and it will be copied over and the blockchain will be restored towards its original value as shown in the figure below.

Fig. 11. A Blockchain restored its original value ©SuperDataScience

This system is secured because the blockchain will continuously be copying itself, except if more than 50% of the network is attacked at the same time and that depends on the system architecture. No one person can do anything on the blockchain network and that was how we bring in “trust” to each other. The technology design bring trust with extra security by the Hash algorithm, the P2P network and the consensus protocol.

The optimized system will build trust through immutable, time-stamped records for keeping track of all voters and preventing double voting due to a developed series of blocks of data, chained together cryptographically using the “hashes”, the integrity is protected by digital signatures for the Blockchain-based electoral system which, “proof of identity” for voters who secured valid voter’s card profiling into the chain. As a peer-to-peer network, combined with a distributed time-stamping server, Blockchain databases can be managed autonomously to exchange information between disparate parties. “There’s no need for an administrator. In effect, the Blockchain users are the administrator (Lucas Mearian, 2018).

1. **How the Mining Works**

A block stores multiple of transactions, so several transactions get pulled into a block. Also in the block we have got the Hash of the previous block and this is a very important feature to be integrated into Blockchain-based Electoral System for Nigeria because that’s how the cryptographic link is facilitated between them.

And finally we have got the Hash of the current block. We got the Hash when we take the Block number, the Data and the previous Hash putting all of that into the Hashing Algorithm and it put out a Hash for us. There is actually another field in the block, the field is called “Nonce”, and “Nonce” stands for “Number Used Only Once”. And this field is what mining is all about. See figure below.

Fig. 12. How the mining works

Eniola -> Ishola \*\* years’ old

Address -> 54 Nomansland, Kano

Mobile -> +234703698\*\*\*\*

8AI49F129D80BFC3AE

5D239F124D817B33F8

#2

Based on the ongoing proposition at Kings Embedded Solutions, we are carefully looking into the protection of data being captured and accessed during voting, its processes, database, and reports on data collated and announced after various elections, validations and accreditations of voters requires diligent. At present, we have identified various solutions that are obtainable on the proposed Blockchain-based electoral system that could manage multiple identifiers for various identities validation and accreditation. With the target to employ voter’s identity management will optimize the present electoral system and will certainly improve the overall efficiency of the system as well, the voters can verify their voting choices using the voters card as a private key at any point in time. By way of integrating an identity on a Blockchain-based electoral system will give the voters a better control over who has their personal information at hand and how they could access that personal information such as the national identity card, international passport, and voters card etc.

The “Nonce” gives us extra control. It gives us extra flexibility. Now we can manipulate the Hash value by changing the “Nonce”. So we don’t have to change the block number because the block number is the block number, we can’t change the previous Hash because it is linked directly to what we have in the previous block. And we can’t change the data because that would mean we are tampering with data and that would defeat the purpose of a blockchain. It has to be an immutable ledger. We want to prevent tampering. Now that we have the “Nonce”, we are free to change the value, since the “Nonce” is just basically a number. That will allow us to be able to manipulate the Hash, to vary the Hash. We cannot control the Hash but we can vary the Hash by varying the “Nonce”. As we vary the “Nonce” in this case, as the voters adds their votes, the nonce changes, thereby varying the Hash dramatically, and this is happening because of the Avalanches Effect in action. It is happening because in the block itself, it certain we can only change a bit of one set of information. Nonce is a number that could go up to billion something. It quite a large number that could accommodate lots of voters.

1. **Byzantine Fault Tolerance**

The byzantine fault tolerance is a very interesting concept that we introduced into the blockchain-based electoral system. It is not used only for blockchain but for any type of decentralize system. The byzantine fault tolerance brought about an algorithm that everybody must agree to advance in order for this to work. This Algorithm is a complex problem which requires an in-depth mathematical proof towards which includes, looking into the messages the majority gets and based their decision on that.

In this case, we are going to relate what the INEC specifics with the Byzantine general problem giving the parties to come into a consensus. Having the INEC to give these specifics for voting to all parties, the voters votes for their respective party choices and vice-versa.

By employing the Byzantine Fault Tolerance to our blockchain-based electoral system and for this Algorithm to work we must have not more than 33% election manipulator/attackers, meaning more than one-third cannot manipulate the election system. There is that, for the blockchain-based electoral system, we might have somebody trying to attack the system and we need to come up with a consensus protocol like an algorithm which will allow us to protect the system from fraud, rigging, election manipulators or from people trying to affect it. We want to make sure the system is tolerant as much as possible, to make sure is not just tolerant to one attacker but to be tolerant to many that may want to attack the electoral system.

1. **The Consensus Protocol: The Defense Against Attackers**

We aimed to solve two main challenges using the Consensus Protocol for the blockchain-based electoral system.

1. The challenge to protect the network from the attackers.
2. The challenge of competing chains.

In a large blockchain systems because it is distributed across the world and there could be a lag especially to a node that are far away from each other. For our blockchain-based electoral systems, it needs to be consensus in order to keep growing as the voters place their votes. If the consensus protocol is not in place, what happens is we will have a conflicting chain thereby resulting to splitting of the blockchain till we have no more blockchain.

In terms of the consensus protocol, there are multiple of consensus protocols as shown in the figure below. We selected to use the Proof-of-Work (PoW) because that is the original described in the Satoshi Nakamoto paper and also it’s the one that bit coin currently uses and it is also the one that Ethereum still uses.

Fig. 13. Types of Consensus Protocols

“Moving even further from trust averse systems, we have private networks that are not only permissioned but also restrict who can see the Blockchain” (Lucas Mearian, 2018). Within the Blockchain, trust relies on the safekeeping of private keys in this the voters card which relies on voters to secure their private key.

**SECURITY**

1. Security is not just about confidentiality, but includes integrity (not corrupted or deleted), availability (able to be accessed when desired), and non-repudiation (once established, cannot be revoked or denied).
2. Integrity: Maintain hashes of device firmware and software records in a Blockchain distributed ledger, so they can be checked to detect tampering
3. Availability: Blockchain distributed ledgers tend to be robust – if one node is damaged or removed, the data persists in the other nodes.
4. Non-repudiation: data recorded in a Blockchain ledger becomes an immutable record – it cannot be changed or deleted (David Snyder, 42TEK, Inc. 2017).

**RESULTS AND DISCUSSION SECTION**

A statement was made in other to tie this with the blockchain mining, that, “A Hash is a number”. A Hash is actually a hexadecimal number – from 0 - 9, and also from A – F. We could come up with a pool of Hashes, starting from the “Smallest value” to “Largest value”. The block is only accepted to the blockchain when the hash is below the system. With the Avalanche Effect, it prevents voters from cheating the system. The reason as for using the Hash Algorithm is because you cannot reverse engineering, you cannot crack it and predict what hash you will get based on the nonce you input. The SHA25 promises that nobody will be able to crack it. SHA1, MD1 and MD5 has been cracked successfully but SHA256 cannot be cracked. A lot of people have tried it; they are not successful.

1. Verify -Voters using the proposed blockchain system can verify their voting choices using their private keys at any point in time, see figure 14 below.

Figure 14. INEC Blockchain-based Voters Login Page

1. Display - Various election results are displayed upon selecting the exact result you want to view such as the Presidential, Governorship, Senatorial, House of Reps, LGA Chairman etc. according to state and election year. See figure 15 below.

Figure 15. Public Voting Choices & Consensus Process.

1. The entire voting system is decentralized which means that information is stored in computers around the world, and is constantly updated in real time to reflect changes in voting and accounts by bringing records together with blocks chronologically for all parties.

Figure 16. Designed Block for All Contesting Parties.

1. Votes are owned by the identities which are the public keys.
2. The integrity of the system is protected by secured hashes

With the Byzantine Fault Tolerance being used in many other places such as Airplanes etc. we could have all the electoral systems in place, talking to each other, and enabling voter’s votes coming through from different distributed networks in the 36 states, we can’t just let the entire electoral system crash because one system from another state or the FCT (INEC Headquarters) failed/attacked. Using the Consensus Protocol, every single node before the blocks is added, will conduct series of checks. And these series of checks are very rigorous. What happens when two voters, votes for the same party candidate, almost the same time. Now we have got a conflict, and have to resolve the argument in the chain where the consensus protocol added best to it very in a very similar way to the Byzantine Fault Tolerance. This is also the Byzantine General Protocol. As shown in the figure below; The consensus protocol looked into the average of the messages the chains are getting by means of the hashing power, if its more 50% that chain eventually wins.

Fig. 17. Consensus Protocol – Block Checks

The consensus protocol checks the list, see the table 1 below for the developed framework for the blockchain-based electoral system.

|  |  |
| --- | --- |
| **S/N** | **Check Lists** |
|  | Check syntactic correctness |
|  | Reject if duplicate of block we have in any of the contestants categories |
|  | The voters list must be non-empty |
|  | Block hash must satisfy INEC Proof-of-Work |
|  | Fast voting be thumb printing (i.e. for the party contestants), the rest must not be thumb printing. |
|  | Check if previous block (matching previous hash) it in main branch or side branches, |
|  | Verify voters’ signatures for each input, reject if any are bad |

Table 1. Developed Check List.

**ADVANTAGES**

1. The potential advantages are that, with the integration of blockchain-based technology solution into the existing electoral systems, voters will be able to verify their voting choices using their voters card as a private key at any point in time.
2. All results could be processed within couple of minutes.
3. It is auditable by the general public.
4. The entire election process will be transparent and decentralized.
5. Everyone participating can see the blocks and the votes stored in them and it’s public which is a great advantage of the blockchain-based electoral system. However, that doesn’t mean everyone can see the actual content of the electoral process; that information is protected by a private key.
6. With the blockchain-based technology solution into the Nigeria electoral process, the systems are decentralized, so no single authority can approve vote or set specific rules to have election accepted after reaching a consensus based on set rules for voting. As a result, the model involves a great deal of trust, as all the voters participating in the network must reach a consensus to accept elections.
7. Most important of all, it’s secure. The database can only be extended; previous records cannot be changed or, at least, there’s a very high cost if someone wants to alter previous records.
8. The proposed technology completely removes paper works or is reduced to about 1% for proper handling over of equipment and other election materials as there won’t be any paper validation.

**LIMITATIONS**

1. The integration of the existing voters card into the blockchain-backed solution for convenient and secure online voting and the entire blockchain architecture for the desired purpose requires an ample of time for the one full development and deployments.
2. We have to generate digital keys for all voters/individuals having issued the voters card to capture the existing card data, which could be resulted to the re-insurances of a new card.
3. There is more innovation to voting technology and these could be fully integrated to optimized the centralized system into a more secured and decentralized systems.
4. There could be some challenges in validating voters after they have voted/casted their votes.
5. The proposed INEC blockchain-based systems for adoption is expected to be slow and steady, as it changes, it gains momentum, and required large energy consumption.
6. The National and Educational adoption.
7. Control, Security and Privacy.

**POSSIBLE APPLICATIONS**

Blockchain applications beyond currency are shown in the figure below:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Figure 6. Application (Nitin Gaur, 2015)

**CONCLUSION**

Our results uncover the engineering ideas behind the blockchain and the ethereum technologies. Our proposition will have the Byzantine characteristics for tolerance. With the byzantine fault tolerance, it is huge concept, very simple in terms of decentralize systems. Also by employing the Proof-of-Work (PoW), every single mode before the blocks is added will conduct series of checks and this series of checks is very rigorous.

The most important conclusion is that in the proposed blockchain-based electoral system, the Consensus Protocol looks into the average with more than 50% of the hashing power, and that chain wins. More than 50% of the blockchain comes into consensus to win. And the key here is that, the part of the network that has the highest hashing power will eventually generate the longest chain and chain wins.

The public blockchain allows anyone to see or send votes as long as they are part of the consensus process. Every voter can go to the polling unit/the online voting portal to log in with their INEC voters card and digital IDs to access the e-voting results.

# **REFERENCES**

1. Bronworth, A., 2016. *MIT License.* [Online]   
   Available at: https://www.github.com/anders94/blockchain-demo/blob/master/LICENSE.  
   [Accessed 2018].
2. Buterin, V., 2017. *The Meaning of Decentralization.* [Online]   
   Available at: https://www.medium.com/@vitalikbuterin/the-meaning of decentralization-a0c92b76a274  
   [Accessed 2018].
3. Christ Berg, S. D. a. J. P., 2017. *The Blockcain Economy: A Beginner’s Guide to Institutional Cryptoeconomics.* [Online]   
   Available at: https://www.medium.com/@cryptoeconomics/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2fbeec  
   [Accessed July 2018].
4. Ebiri, K., 2016. *The Guardian News, How Card Readers Were Manipulated by INEC.* [Online]   
   Available at: https://www.guardia.ng/news/how-cardreaders-were-manipulated-by-inec  
   [Accessed May 2018].
5. Feig, E., 2018. *A frame for Blockchain- Based Application.* [Online]   
   Available at: researchgate.net/Publication/323549800, pg. 3.
6. Gaur, N., 2015. *Presentation: Making Blockchain Real for Business.* s.l., s.n.
7. Hadelin, K. a., 2018. *Blockchain A-Z Course, Super Data Science,.* [Online]   
   Available at: https://www.superdatascience.com.  
   [Accessed 28 May 2018].
8. INEC, 2017. *INEC Card Reader - Wikipedia, the free Encyclopedia.* [Online]   
   Available at: https://en.wikipedia.org/wiki/INEC\_card\_reader  
   [Accessed May 2018].
9. INEC, 2018. *INEC Statement on Card Reader Demonstration.* [Online]   
   Available at: http://www.inecnigeria.org/?inecnews=inec-statement-on-card-reader-demonstration  
   [Accessed 25 July 2018].
10. Lakhani, K., 2000. *.* s.l., Harvard Business school. pg. 5..
11. Leslie Lamport, R. S. a. M. P., 1982. *The Byzantine Generals Problem.* [Online]   
    Available at: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.  
    [Accessed 2018].
12. Mearian, L., 2018. *What is Blockchain. The Most Disruptive Tech in Decades, Senior Reporter.* s.l., Computerworld, pg. 26.
13. Nachiappan, M. C. a., 2015. *Blockchain Technology Beyond Bitcoin.* s.l., Sutardja center for Entrepreneurship and Technology, Berkeley Engineering, Pg.12.
14. Nakamoto, S., 2002. *Bitcoin: A peer-to-peer Electronic Cash System.* [Online]   
    Available at: http://www.hashcash.org/papers/hashcash.pdf  
    [Accessed 12 July 2018].
15. Nakamoto, S., 2008. *Bitcoin P2P-Cash Paper,.* [Online]   
    Available at: http://www.moril-achieve.com/cryptography@metzdowd.com/msgo9997.html  
    [Accessed August 2018].
16. Researchers, 2018. *INEC Nigeria.* [Online]   
    Available at: http://www.inecnigeria.org/?page\_id=797  
    [Accessed May 2018].
17. Snyder, D., 2017. *Blockchain Technology for the Internet of Things.* s.l., Presuder 42TEK, Inc. Pg. 12..
18. Stornetta, S. H. a. W. S., 1991. *How to Time- Stamp a Digital Document,.* [Online]   
    Available at: https://www.anf.es/pdf/Haber\_Stornetta.pdf  
    [Accessed July 2018].
19. Swan, M., 2015. *Blueprint for a New Economy from Blockchain.* s.l., https:// Blueprint for a New Economy from Blockchain, pg.34.
20. Thieau, M. P. a. D., 2018. *IBM Developers Works.* [Online]   
    Available at: IBM Blockchain 101, quick-start guide for developers, http://www.ibm.com/developerworks/cloud/library/cl-ibm-blockchain=101quick-start-guide for developers.  
    [Accessed 26 May 2018].
21. Veness, C., 2017. *Morable Type Scripts,.* [Online]   
    Available at: https://www.movable type.co.uk/scripts/sha256.html.  
    [Accessed 12 July 2018].
22. Werkhaven, W. P. a. V., 2008. *On the Secure Hash Algorithm Family (chapter 1 of cryptography in context).* [Online]   
    Available at: https://www.stuff.science.uu.nl/~tel 00101/liter/books/cryp cont.pdf.  
    [Accessed July 2018].