A Blockchain based Algorithm for Electronic Voting System

Omogbhemhe M.I.
Ambrose Alli University, Ekpoma

ABSTRACT
The lack of fidelity in the present system of voting has made many researchers to advocate for a better system. This has resulted in developing peer-to-peer version of election voting system like the online voting system. This system would allow online voting to be done without the need of worrying about the authenticity of the result generated. This kind of digital signatures provide part of the solution, but the main benefits are lost if the verification and counting of the votes are entrusted to an organization. This paper proposed a solution to the counting and result authenticity problem faced while using the peer-to-peer system of voting that must be manage by a single organization. The solution is the development of a blockchain based voting system to achieving optimal vote's fidelity in the election after voting. The network timestamps votes by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be altered without redoing the proof-of-work**.**

Keywords
Blockchain, Algorithm, Voting, Technology

1. INTRODUCTION
Elections in Nigeria are forms of choosing representatives to the Nigerian Federal government and the various states in the fourth republic Nigeria. Nigeria voting system uses an open ballot system, is a voting method in which voters vote openly by queuing or otherwise, indicating the candidate of their choice. In modern times, the open ballot was first adopted in the Third Nigerian Republic during the 1993 Nigerian presidential election, an election that was widely regarded as the freest and fairest in the country's political history (TVC News, 2016). The open ballot system or the option A4 is not a good way of voting in Nigeria. The system does not assure Nigerians that their votes are been counted. Result of votes are verified by an organization (INEC) which can be maneuvered and the suppose party chosen by the people loses the election. In the open ballot system the elections can be rigged in different ways: Militarizing of opponent's area, Ensure late arrival materials in rival's polling unit, Threaten of INEC officials, Compromising INEC's logistic process, Compromising INEC officials, Snatching of ballot boxes/papers in rival's polling unit, Electoral violence/thuggery, Manipulating results at collation centers, Vote buying [1]. All the aforementioned ways of rigging are done in the Nigeria's open ballot elections which falsify the result of the votes, and also bring risk to Nigerians life. In the just concluded elections for instance, there were report of clashes between army officials and suspected thugs, nine persons were reportedly killed including a soldier [1]. These problems can be solved by introducing an electronic voting system, but an electronic voting system which uses a normal database can be hacked by hackers which doesn't solve the whole problem (the system can still be rigged). What is needed is an electronic voting system based on blockchain technology, a system that can't be hacked. Blockchain was invented in 2008 by pseudonymous Satoshi Nakamoto to manage Bitcoin, a crypto currency network. Blockchain is an algorithm designed free of any agencies, mainly to manage electronic information without any central administrator [2]. Since, no central of administrator, implementation of blockchain is transparency and cannot be tampered. Blockchain does give user anonymity because no personal identifiable information is exposed directly in a block. Blockchain based e-voting should preserve its security and privacy on a high-level scale. Introducing blockchain technology into Nigeria's voting system can strengthen the security of voting process, protect the privacy and protect the life of each voter. The blockchain based e-voting system is decentralized and does not need to rely on human trust. Registered voters have the right to vote using their electronic devices connected to the Internet. All the vote records will be publicly distributed and can be verified by any intended personnel. No one is able to corrupt this kind of voting process.

Blockchain Technology

Blockchain is a growing list of records, called blocks that are linked using cryptography [3]. Each block in the blockchain contains the timestamp, the previous cryptographic hash and the data.

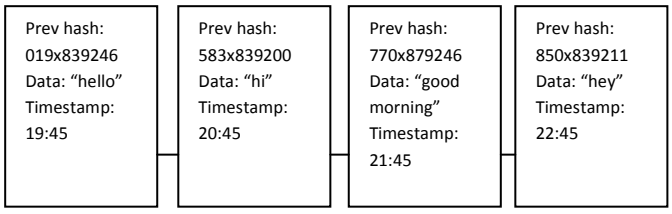

Fig 2.1 A Blockchain

The diagram depicted above gives an example of blockchain which contains the time the block was created and the hash of the previous block, and the data it holds. The data in a block can't be edited. It is an append-only data structure. Any block added into the blockchain can't be manipulated. By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way" [4]. A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter node communication and validating new blocks. Once recorded, the data cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. The data structure can't be edited without the agreement of the network majority; it uses a decentralized, distributed, and public ledger which prevents the altering of

data in the block. Each node in the blockchain contains a copy of all the blockchain, when a change is done, or a block is added it synchronizes to all the nodes in the network and everyone sees it. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks [5].

Using the voting system as an example; when a civilian votes, it is synchronized to the whole network and it is confirmed.

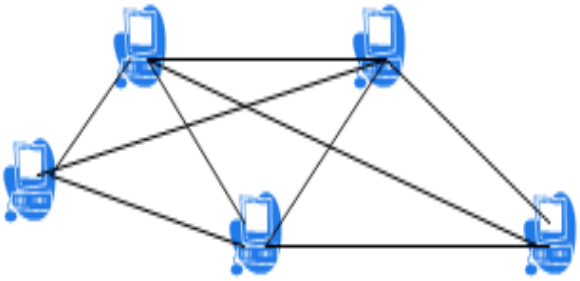

Fig 2.2: Decentralized Network

Fig 2.2: Centralized Network

Once the vote is confirmed to agree with the rules in the network it is added to the blockchain. The process of adding a block to a blockchain is called mining. This is done by miners, they solve computational puzzle to create a block and they are rewarded. With this technology used in the Nigeria voting system the votes of the people can't be changed and the result will be trusted.

Technologies used in Blockchain

There are four particular technologies which are used to enable blockchain:

Asymmetric Key Encryption: this is also known as a private-public key encryption, which serves to create user identities in the blockchain. A user in the blockchain owns a private key and a public key. Asymmetric encryption allows for the authentication of users because only those with the private key can decrypt data encrypted with the public key or encrypt the data for public key decryption, thereby creating a signature.

Hash Values: this is used to validate the block's integrity. The hash value is created by mathematical functions as an encryption method to produce a string of characters as an output given some data as input. Any alteration in the data in the block will change the hash value. It enables users on the blockchain to determine whether or not they can trust the history of data on the blockchain.

Peer-to-Peer Networks: this is decentralized network. It allows users to be connected together without any central authority. This is adopted in the blockchain technology which enables users to be connected together and have a copy of the whole blockchain.

Merkle Trees: it is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. It allows efficient and secure verification of the contents of large data structure.

Classification of Blockchain Systems

The blockchain system is classified into three:

Public Blockchain: as the name implies, it provides a platform to the public. Anybody can join, mine and transact. These are also called "permission-less" blockchains [6]. Every node in this platform is given full authority to read/write.

Private Blockchain: this is the opposite of the public blockchain. It only gives the full authority to a specified group of persons. An unauthorized person can read/write in the blockchain.

Consortium Blockchain: this is a hybrid blockchain. It is partially private and partially public. The permission are been controlled by some group of persons.

Characteristics of a Blockchain

According to [7], every blockchain has the following characteristics

Consensus: For a transaction to be accepted and recorded on the blockchain, all the participants must agree to follow the same rules. If a transaction violates one of the rules the network agreed on, the transaction will be considered invalid. The consensus allows each participant to trust the network, because they know each transaction will follow rules they ratified when the network lauched.

Provenance: participants know where the assets came from and how its ownership has changed over time. If we have a blockchain designed for a voting system, it must be known where it is coming from, by whom, and when.

Immutability: no participant can modify a transaction after it has been recorded on the ledger. There is no higher authority, every node present in the network has equal right, after the vote have been recorded it can be changed except by re-hashing the whole block which would take high computation power for just a node.

Finality: in a blockchain network, there is only one source of truth. There is only one ledger for the whole network. To know who owns what, or to study a particular vote, there is only one place to go.

Methodology

The major sources used to gather information and the tools used in this paper are stated as follows.

The use of the Internet: The use of the internet which is the

best source centre was of great importance in the achievement of this seminar. Various website were visited to extract relevant materials related to this seminar work.

Development tools: In the achievement of this seminar work, many tools were put together, some of the tools include JAVA, which was used as the selected programming language, blockchain technology for the database, and Android Studio for the design of the interface.

2. E-VOTING BLOCKCHAIN ALGORITHM

In this section the algorithms used in the e-voting system are given. The algorithms are written in Java programming language. Software engineering principles were adopted in developing this system, breaking the development of the application into modules (functions). Each function performs a particular operation in the e-voting system. The software engineering principles were adopted to make the application easy to read and not complex for debugging.

Verification of PVC

There could be scenarios where the permanent voter's card (PVC) information given may be false or not valid, the algorithm given below solves this problem.

```
public static boolean verificationOfPvc(String VIN, String [] vinList) {
        for(int i = 0; i < vinList.length; i++) {
            if(VIN == vinList[i]) {
                return true;
            }
        }
        return false;

    }
```

In the above algorithm, the function *verificationOfPvc*(a, b) has two parameters which takes in arguments. The first parameter takes in a string of numbers (VIN), the second parameter takes in an array of strings (this comprises of every VIN in the blockchain). The algorithm takes the first parameter and checks if it is valid by scanning through the list of VINs to see if the VIN exists in the list. If the VIN is valid it returns true else it returns false.

Creation of Ballot ID

Ballot Identity is given to voters after the voter's details have been verified using the above algorithm. The ballot ID creation problem is solved with the algorithm given below.

```
public static String applySha256(String input) {
        try {
            MessageDigest digest = MessageDigest.getInstance("SHA-256");
            //Applies sha256 to our input.
            byte[] hash = digest.digest(input.getBytes("UTF-8"));
            StringBuffer hexString = new StringBuffer(); //This will contain hash as hexidecmal
            for(int i = 0; i < hash.length; i++) {
                String hex = Integer.toHexString(0xff & hash[i]);
                if(hex.length() == 1) hexString.append('0');
                hexString.append(hex);
            }
            return hexString.toString();
        }
        catch(Exception e) {
            throw new RuntimeException(e);
        }
    }
```

The above algorithm is called sha256. Bitcoin uses this algorithm to solve the hash code of each block when creating new blocks. In this section the algorithm is used to create ballot ID for voters. The output of this algorithm can never be linked back to the user. This takes in the surname of the voter and the VIN and creates a ballot ID.

```
public static String creatBallotID(String surname, String VIN) {
        return applySha256(surname + VIN);
    }
```

The code above uses the sha256 algorithm discussed earlier, it combines the two parameters it has (surname and VIN) and returns a ballot ID.

Registering of Ballot ID

Registering the ballot ID is done to prevent a user to register more than once in the network, and it also prevents hackers from voting with unregistered ballot ID. It is only registered ballot IDs that are allowed to vote. This seminar uses a blockchain to store the registered Ballot ID which prevents the ballot ID to be changed.

```
public class Block {

    public String hash;
    public String previousHash;
    private String data;
    private long timeStamp;


    public Block(String data, String previousHash) {
        this.data = data;
        this.previousHash = previousHash;
        this.timeStamp = new Date().getTime();
        this.hash = calculateHash();
    }
    public String calculateHash() {
        String calculatedhash = StringUtil.applySha256(previousHash + Long.toString(timeStamp) + data);

        return calculatedhash;
    }
```

The code above creates a class, from this class objects can be created. Each object created from this class has the attributes of the class. In this section the data variable is going have the value of the ballot ID. In creating a block sha256 is used to calculate the hash code.

```
    public static ArrayList<Block> registeredBallotID = new ArrayList<Block>();
```

```
public static void registerBallotID(String ballotId,
String [] listBallotID, Block newBallotID) {
        if(ifBallotIDRegis(ballotId, listBallotID))

registeredBallotID.add(newBallotID);
}
```

An array list was created to hold the new registered ballot ID. Whenever a block is been created the block contains the ballot ID, the time it was created, the previous hash code, and the current hash code. The current hash code is calculated by hashing the Ballot ID, the time it was created, and the previous hash code together. This is a technique used in the blockchain technology which prevents the data from been changed.

Voting

```
public class contestant {
private static long vote = 0;
public contestant() {
        this.vote = 0;
}
public static void add() {
        vote += 1;
}
public static long get() {
        return vote;
}
}
```

All contestants are created from this class. The vote variable is made private so no unauthorized person can change the value. The add function is used to increase the contestant vote when a voter votes, and the get function is used to return the number of vote a contestant have.

```
public static void vote(String ballotID, String []
listBallotID, contestant cont) {
        if(ifBallotIDRegis(ballotID, listBallotID))
                cont.add();
}
```

The function above checks if the ballot ID is registered, if it is registered it adds the vote to the contestant.

3. PROPERTIES OF PROPOSED BLOCKCHAIN BASED E-VOTING PROTOCOL

Authentication: Our system only accepts registered voter to cast their vote. Our proposed system is able to verify voters' identities against their previously registered credentials and let only allow them to vote once. Identity fraud is prevented. These properties are supported by digital signature in blockchain. Digital signature is an asymmetric encryption process where the key pair required is mathematical associated with each other. The signature is included in the ballot block so anyone can proof that only the sender could have cast the particular vote using the sender's public key. Every ballot block on blockchain is digitally signed by the sender using their private key during the registration phase and ballot casting phase.

Integrity: The entire vote received by the system must be accurate, and every vote casted must be counted and cannot be duplicated or changed or removed. Any tampering of the ballot should be detected by the proposed system and immediately flag the malicious vote. The integrity of vote is supported by hashing technology in blockchain. SHA-256 algorithm hashing is used and will always produce an output of 256-bits. Hash is used to verify that either any ballot block has been tampered in way that is not intended. Every ballot block is added and hashed in sequence. For every new ballot block generated, every previous block hash, and the current ballot information is used as an input to determine the latest block hash. This cycle has form a sequential linked chain of block hash. This guarantees the integrity of each block as it would be fairly easy to detect any tampering of vote.

Publicly Verifiable: Everyone participants involved in the election or non-involvement parties can see the voting process and verify all the votes if they are intended to do so. The outcome of the election will have total transparency after the election finish.

Voter Pseudonymity: Although the voting result chain is publicly shared, only the voter themselves can know their own ballot belonging. They only have access to the vote result but have no unique information to connect the result with any voters. This serves to protect the voter identity as this proposed system able to prevent other from knowing who the voter casted their vote for.

Result consensus: Properties supported by the consensus mechanisms of blockchain technology, where all the participants involved hold the same record of the voting result and accept the same outcome of the election without rely on any central authority. Everyone reaches a general acceptance of election outcome. This prevents any dispute of disagreement regarding the election outcome as the voting result is fair and transparent.

Availability: The proposed system should be implemented easily across the country and it should be accessible to most of the population. Voter can check for the eligibility of votes anytime they want after the election process end. This system architecture is suitable to be used in both mobile app and any computational device that connected to the Internet.

4. CONCLUSION

The proposed algorithm/system uses a technology known as blockchain which comprises of other technologies. This system was proposed to improve the current voting system. This system increases the security and authenticity of the votes and it builds the voters trust on the integrity of the electoral system. The system shows the result of the elections till the very end of it. It uses a peer-to-peer (P2P) network which enables all users to know any changes made in the system. The system does not rely on human trust but on computational cryptographic trust

5. REFERENCES

[1] Queensther I.(2019). 10 Ways that Politician rig ElectionsinNigeria.fromhttps://www.google.com/amp/s/www.premiumtimesng.com/features-and-interviews/318339-10-ways-politicians-rig-elections-in-nigeria.html%3famp_markup=1

[2] Hoffstein, J, Pipher, J, and Silveran, J. H, (2008) "An Introduction to Cryptography". Springer Science+Business Media. vol. XVI: 1 - 24.

[3] Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. (2016) "Bitcoin and cryptocurrency technologies: a comprehensive introduction". Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[4] Lansiti, M.; Lakhani, K. R. (2017) "The Truth About Blockchain". Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

[5] Armstrong, S. (2016) "Move over Bitcoin, the blockchain is only just getting started". Retrieved from https://www.linux.com/news/move-over-bitcoin-blockchain-only-just-getting-started.

[6] Puthal, D.; Nisha, M.; Saruju, P. M.; Elias, K.; Gautam D. (2017) "Everything you Wanted to Know about the Blockchain". Retrieved from http://www.smohanty.org/Publications_Journals/2018/Mohanty_IEEE-CEM_2018-Jul_Blockchain.pdf.

[7] Damien, C. (2018) "The 4 Characteristics of a blockchain". Retrieved from https://dev.to/damcosset/the-4-characteristics-of-a-blockchain-2c55.