**Full Paper**

**A FRAMEWORK FOR ELECTRONIC VOTING SYSTEMS USING BLOCKCHAIN TECHNOLOGIES**

**Kasali, Funmilayo A.**

Mountain Top University, Ibafo,

Ogun State, Nigeria

fkasali@mtu.edu.ng

**Orah, Richard O.**

New Horizon Solutions,

Nigeria

orahseun@gmail.com

**Balogun, Jeremiah A.**

Mountain Top University, Ibafo,

Ogun State, Nigeria

jabalogun@mtu.edu.ng

**Aleburu, Deborah D**

Mountain Top University, Ibafo,

Ogun State, Nigeria

ddaleburu@mtu.edu.ng

**Igiri, Chinwe P.**

Mountain Top University, Ibafo,

Ogun State, Nigeria

cpigiri@mtu.edu.ng

**Adekola, Olubukola D..**

Babcock University, Ilisan,

Ogun State, Nigeria

adekolao@babcock.edu.ng

**Sani, Felix A.**

ayegba.sani-felix@binghamuni.edu.ng

ABSTRACT

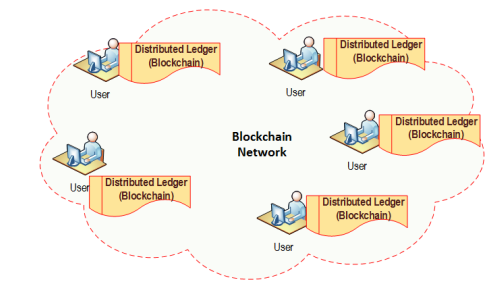
In recent years, blockchain technology has been widely applied in the development of immutable and trustworthy solutions for different application areas. The traditional use of ballot boxes for election is gradually being overtaken by online voting to limit the issues of violence and malpractices in the electoral process but the risk involved in this method can be devastating in case of any loophole in the security of such systems. In this study, we proposed the use of blockchain technology (Ethereum and Smart contracts) with the SHA-256 cryptographic hash algorithm to encrypt users’ data both at the server side and user view for an electronic voting system. We implemented the framework using Java programming language, Netbeans Integrated Development Environment (IDE) as the frontend with MySQL database as the backend. The proof-of-concept applied in this study shows that using blockchain technology can widely enhance the security in such systems, thereby improving the electoral process. In future works, we propose to test more cryptographic algorithms like the Advanced Encryption Standard (AES), Eclipse Curve Cryptographic (ECC) and the SHA 512 hash algorithms on the system. The System Usability Scale (SUS) would be used for empirical analysis with existing systems for comparative analysis basis and to also identify the strengths and limitations of our system with existing systems.

**Keywords:** Block chain, e-voting systems, decentralized systems, SHA-246 Cryptography

1. **INTRODUCTION**

In Nigeria, the electoral process has been marred with numerous challenges which include violence and unnecessary intimidation of voters, snatching of ballot boxes, incomplete and false results, underage voting amongst others (Ahmad, Abdullahb & Arshadc, 2015). The citizens have gotten so fed up of the whole process to the extent that some have given up and rarely go out to vote during elections as a result of lack of transparency and trust in the system (Uzedhe & Okhaifoh, 2016). Paper voting, which has been used for conducting election in Nigeria since 1999, has proven to be not only unsuccessful but also dangerous (Agbu, 2016). In other to achieve a more reliable and transparent election, democratic countries worldwide are now resorting to take advantage of current technological innovations. Examples of such countries include Brazil, India, Australia, Japan, and United States of America amongst numerous others (Esteve, Goldsmith & Turner, 2012). It has been realized that online voting has the tendency of increasing voters turn out rate and also reduce the cost of the whole electoral process (Jafar, Aziz & Shukur, 2021). Electronic voting has the tendency of eliminating most of the challenges of traditional voting systems (Alam & Tamura, 2012). Ejalonibu (2021) opined that for any electoral process or system to have a high level of integrity, the populace or voters should be able to have a high percentage of trust in it. The main problem of most electronic voting systems are the issues of trust, security and how to ensure that voters’ identities remain anonymous (Kucharczyk, 2010). The use of blockchain technology has been explored by numerous researchers and applied in developing applications as a result of its secure, transparent reliable, immutable and decentralized nature in building trustworthy systems (Rouhani & Deters, 2021; Baygin, Baygin & Karakose, 2019). The technology works in a way that members who have no trust in themselves can verifiably relate with themselves without needing any trustworthy authority (Christidis and Devetsikiotis, 2016). Blockchain technology has been implemented in many financial service applications and in providing more security to digital assets (Paech, 2017). It has also been widely applied in integrity verification (Zikratov et al, 2017), governance (Hoy, 2017), in citizenship and user services (Rivera et al, 2017), for Internet of Things (Cassino et al, 2019), security of intellectual properties (Xu et al, 2017), in healthcare management (Juneja et al, 2018), governance especially in minimizing or total elimination of corrupt practices (Hou, 2017), public sector especially in the area of land management and allocation (Pichel, 2016), data management (Jin et al, 2017), supply chain management (Kennedy et al, 2017), business and industrial applications (Ying et al, 2018). The technology has also been applied in education for collecting and analyzing all academic records for efficient decision making processes (Bore et al, 2017) and in electronic voting ((Hsiao, et al, 2018). Despite the numerous benefits of blockchain, the issue of data privacy still persist (Peng et al, 2021). Hence, in this study, we proposed a framework for designing a more secured electronic voting system using blockchain technologies and we improved on existing frameworks by incorporating a customized version of the SHA-256 algorithm, a widely used and one of the most secure data encryption algorithm.

Blockchains are digital ledgers that are implemented in a distributed manner (do not require a central repository) and exist in most cases without a central authority such as a bank, company or government agency (Narayanan, Bonneau, Felten, Miller, & Goldfede, 2016). At a basic level, it allows the users’ community to record transactions using a shared ledger so that, in the normal operation of the blockchain network, no transaction can be changed once it is published (Polge, Robert, & Le Traon, 2020). As shown in Figure 1, blockchain-based technologies are based on the use of a peer-to-peer network framework where no centralized trusted third party is required to manage transactions. A blockchain architecture has three components, namely: Distributed Ledger, Smart Contacts and Distributed Applications (Yaga, Mell, Roby and Scarfone, 2018). The distributed ledger uses a distributed digital ledger technology (DLT), smart contracts provide a way to express transactions stored in the distributed ledger while distributed applications are implemented for the end-users of the blockchain technology.



**Figure 1:** Figure 1: Blockchain technology – distributed ledger technology without a trusted third-party (Rawat, Choudhary, & Doku, 2020)

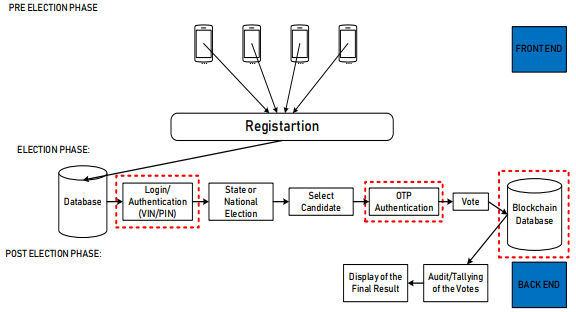
Blockchain networks can be categorized based on their permission model, which determines who can maintain them such as publish blocks (Rawat, Choudhary, & Doku, 2020). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned (Polge, Robert, & Le Traon, 2020). The core characteristics of blockchain technology—decentralization, consistency, integrity, and anonymity - apply to non-financial areas such as smart contracts, the Internet of Things (IoT), reputation systems, security services, wireless virtualization, and other applications. Blockchain has provided protection and safeguarded information against all forms of fraud and data theft hence why it was adopted as the technology for creating financial cryptosystems; the first kind been the Bitcoin (Subramanian & Kamatham, 2019).

Nowadays, with the development of blockchain technology, smart contracts are being constructed as computer programs running on blockchain nodes and can be issued among untrusted, anonymous parties without the involvement of any third party (Ante, 2020; Khan et al, 2021). The first successful implementation of a blockchain-based smart contract was Bitcoin Script, a purposely not-Turing-complete language with a set of simple, pre-defined commands. As simple forms of smart contract, standard types of Bitcoin transactions, such as pay-to-public-key-hash (P2PKH) and pay-to-script-hash (P2SH), are all defined with Bitcoin Script (Antonopoulos, 2014). In addition, there also exist platforms that enable more complex contractual functionalities and flexibilities, e.g., Ethereum, which adopts a Turing-complete language for smart contracts (Wood, 2014). Newer blockchain platforms such as Neo and Hyperledger Fabric allow smart contracts to be written in various high-level languages. However, complexity in the blockchain increases as the size of the network increases thus requiring effective cryptographic algorithms to be implemented. Cryptography is necessary for protecting privileged information when communicating over an unsecured or untrusted medium.

Cryptography makes a message unreadable to a third party, however, it does not hide the existence of the message to the third party (Oke et al, 2019). In most cases, the process of encryption involves the use of an algorithm which is based on a hash function. Hash functions convert an input data string into a numeric string output of fixed length. These algorithms are very effective due to their one-to-one mapping of input string to a unique output numeric string output thus making them collision-resistant. The most popular cryptographic hash function algorithm is the SHA-256 which stands for Secured Hash Algorithm 256.

The SHA started as the SHA-2 which is a set of cryptographic hash functions that was designed in 2001 by the United States National Security Agency (NSA) among which is the SHA-256 hash function. It has a fixed length of 256 bits based on a manipulation detection code instead of a key-based hash function. E-voting can benefit from fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of stored records (Hao, et al., 2014). A detailed analysis of the SHA-256 algorithm and how it works is found in Yoshida & Biryukov (2006). Blockchain technology can play a key role in the domain of electronic voting due to its ability to preserve anonymity, and maintain decentralized and publicly distributed ledger of transactions across all the nodes. This will make blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

Musa & Aliyu (2013) designed a centralized electronic voting system in which the system administrator has the autonomous power of registering voters, counting of election results and declaring the outcome of the process. The limitation of this system is the fear of what could happen if the administrator of such a system gets compromised (Al-madani, Gaikwad, Mahale & Ahmed, 2020). McCorry, Shahandashti, & Hao, (2017) worked on a system that uses a smart contract to implement a voting system is the project by, they created a smart contract for boardroom voting with maximum voter’s privacy. Arshad, & Khan (2018) proposed a blockchain voting system based on Ryan (2008) approach. Hsiao, Tso, Chen and Wu (2018) proposed the idea of a blockchain based e-voting system using homomorphic algorithm but no implementation was done. Yi (2019) designed a blockchain e-voting system based on distributed ledger technology and the Elliptic Curve Cryptography (ECC) for authentication purposes. Ahlkvist et al., (2019), proposed an e-voting system called DeVote that consist of the voterID generator which provides eligible voters with an anonymous ID, and the smart contract. In this system, a voter can always confirm that her vote had been placed and if done correctly. Zhang & Romero (2020) designed a secure e-voting system using Paillier encryption to ensure privacy and availability of data. Khan, Zhang & Lee (2020) gave a detailed analysis of the consensus algorithms used in blockchain technology and opined that the proof-of-work (PoW) algorithm which is used by ethereum consumes the most in terms of computational power and transaction throughput per second but for a system that needs to be highly secured, the PoW algorithm remains more preferable as using any form of permissioned algorithm for building an e-voting system could still lead to security issues since there still remain the fear that some of these validators could be compromised especially in building immutable systems (Malakhov, Marin, Rossi & Smuseva, 2022). In this work, we improved on existing e-voting systems by applying blockchain technology, customizing the SHA-256 cryptographic algorithm and integrating this into the system for enhanced information security.



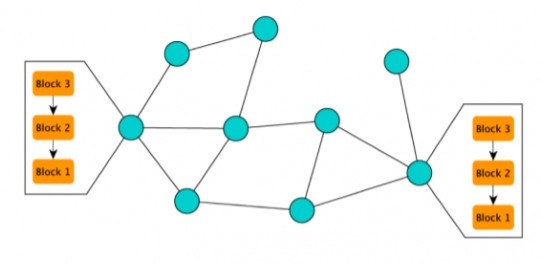
**Figure 2**: Adapted Framework (Abayomi-Zannu et al, 2019)

1. **MATERIALS AND METHODS**

***2.1 Proposed Framework of the Electronic Voting System***

Figure 3 depicts the proposed framework of the e-voting system which is an adaptation of Abayomi-Zannu et al (2019). The adapted framework has a pre-election phase where voters have to register in other to take part in the electoral process and the electoral phase where they get to cast their votes. For registration purposes, information such as Voters Identification number (Voters ID), One time password (OTP) and other details have to be provided and all these are stored in a database. At the backend which is where the blockchain technology is implemented, all the votes that have been casted are stored on the blockchain database and once the election is over, they are counted and results announced. The adapted framework is shown in figure 2.

In our system, the Proof of work (PoW) consensus algorithm was implemented using Java programming language and e-voting was integrated into the block using the SHA-256 encryption algorithm that was customized by inputting the voters information which was converted into an unreadable format to keep voters details secured. Various transactions that can be done by voters are shown in the diagram. The voters can make transactions to Block-2 and start voting. The contract code is written such that once any transaction is received, it will increment the vote and terminate by itself after a while and voting results would be published and saved in the storage space. In the framework, a vote is a transaction and as voters cast their votes, the result is added to the blockchain and voters (users) can see this in real time and also know the number of votes casted for a particular candidate at every point in time. In the framework, information is stored sequentially in blocks with those who have adequate rights to verify and store each transaction otherwise known as validators. The proposed blockchain uses ethereum which is a permissionless based algorithm so voters cannot know who the systems’ validators are and they can be picked among all participating parties in the electoral process. Blockchain is applied in this framework right from the voters’ registration phase, vote storage and counting phases. For any corrupt practices to occur, all validators on the blockchain have to reach some form of consensus which is unlikely as they would not even know themselves. The steps below give a detailed discussion on the architecture in figure 2:



***Figure 4:*** *Version of a blockchain (Dhillon et al, 2020)*

**Step 1**: Defining the constants

In this first step, the input variables such as party names, alongside of difficulty (blocks that ranges from 1 to 5) and the Genesis block would be initialized. Initialization is done based on the Genesis block which is always zero (0)

**STEP 2: Generating Hashes:**

Here, the SHA-256 algorithm is implemented in Java in other to take advantage of the built-in methods and classes of Java security. The procedure involved importing crypto-security in Java and this was used to encrypt the data in the blockchain.

**STEP 3: Creation of Blocks**

Block are created and linked cryptographically using hash values For creating a block, a block class is implemented, and in that class, several variables are defined, such as the Id of the block, the timestamp, the hash of the block, the previous hash in the Blockchain, the transactions, and the nonce.

**Step 4: Implementing Blockchain**

In this step, the blockchain is implemented by storing the generated blocks in an ArrayList.

**Step 5: Miner Approach**

Mining means finding the right hash value to encrypt a particular block. This is done to secure and verify each transactions. Although there exists some constraints as far as difficulty is concerned but every miner is going to get a reward for validating the given transactions. During the coding process, we defined the difficulty as '5', which means there has to be five leading zeros at the beginning of every hash. So, miners would have to generate hash values until they find the right hash. In this work, miner’s reward is 30.0 bitcoin.

Basically, blockchain is a system such that users can send information to one another in a decentralized pattern in a way that user A can send information to User B and User B can send information to User C which makes it an end-to-end transaction. It is a secured technology because information gotten are not stored in any centralized storage system. It is a form of digital ledger that ensures that all nodes on the blocks are counted for a particular voters. The SHA-256 algorithm ensures that each voters’ record is encrypted in such a way that once information enters the block, it gets the hash attention and then gets encrypted.

The blockchain database ensures that each transaction cannot be corrupted and can easily be verified. Voters’ records cannot be tampered with because they do not exist in a single place on the network. The technology allows voters to ensure that their votes are counted and recorded accordingly without any form of ballot compromise. Control and verification of election outcome is done by many trusted voting officials and hence, improving voters trust in the whole electoral process. In figure 4, the circles denotes validators (nodes) in a network and the rectangle represents three blocks in a chain. For any manipulation or fraud to take place in such a network, it means that all the nodes have to reach a form of consensus which makes it a better way of securing information.

**2.2 E-VOTING SYSTEM REQUIREMENTS**.

* The system should allow users to cast votes on various election instances.
* The system should allow only authenticated and authorized users to cast votes on authorized electoral instances.
* Factory Elections should create multiple instances of other elections.
* Election Instances should allow users to vote for their preferred candidates.
* Users should be able to register on the system.
* If election instances are still made available, authorized users should vote.
* Election instances should not allow users to vote if the instance has been ended or closed.
* Voters can select between authorized election instances to vote in.
* Voters can choose from a list of options of available candidates to vote for.
* Each election instance should contain certain unique variables and functions that specify each electoral flow.

Each user should have a system-generated voter Id after registration has been made successfully.

In this e-voting system, the chairman is the systems administrator who is in charge of registering voters for the electoral process. It is expected that voters would have registered to vote using their information such as National Identification Number (NIN), full names, date of birth, place of residence, email address amongst others. After these information have been provided, the system would now generate a username and One Time Password (OTP) for voters which will be used to access the system on the day of election. The generated password and Voter identification number would not be visible to the administrator as this would have been encrypted by the SHA-256 customized algorithm thereby ensuring total security and anonymity of voters. The chairman of the electoral process is in charge of coordinating voters during registration, can create an election instance amongst other roles as indicated in figure 3 and figure 4 respectively. The admin can also create a factory instance of the smart contract being created. The use of a factory contract is to create multiple instances of an electoral process, this being the case that the one who creates the instance of this contract becomes a chairman or the official. In each case of a deployed election instance, at least two candidates must be initialized with such instance in other to allow users to choose from the options made available to them.

**2.4 E-Voting System Flow Chart Diagram**

Figure 8 depicts the sequential steps of the system process using the two system actors. The system takes input from the voter and the admin, representing the potential steps that each actor could take, and the end and final step of each process.

The system consist of both the administrator voters as main actors of the e-voting system.

**Admin Login:** The admin will login with username and password for authentication purposes provided that, the username and password is valid else access would be denied

**Admin create Voter Account:** The admin is able create account for eligible voters once they have access to the system and they can vote for any candidate of their choice.

**Admin update:** System administrators can do updates in special cases but they cannot perform any update action on voters ID or any other voters’ information, they can only do updates in cases where voters forget their login details. At this point the admin can allow the user have access to the system in such a way that an update can be done on their page based on previous information submitted like the NIN.

**Admin View the Result**: Admin also have access to view outcome of elections. Decrypted plain results are visible for admin while encrypted results are visible to voters and party candidates.

**Hash Function:** The application results are based on hash function and this is the benefit of applying blockchain technology as the result are only visible for authorized users.

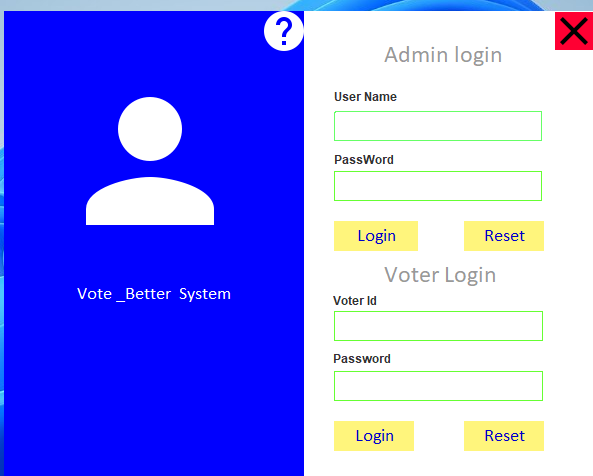
Voters can also access the system with their username and password, they can only vote once if found eligible for any candidate of their choice. They can also modify their or change their votes as long as the election is still open.

**3. RESULTS AND DISCUSSION**

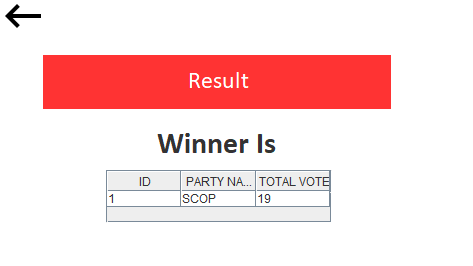
**The framework was implemented with MySQL local server for the backend, NetBeans IDE for frontend. The SHA-256 algorithm was implemented in Java. The system has various stages of results at each level of the block. Block-2 was used in implementing the voting system while Block-4 was used to implement the outcome of the electoral process while other blocks are responsible for encryption of the data which can only be visible to the system admin. Figures 9, 10, 11, 12 and figure 13 depicts the interphase of the electronic voting system after implementing the framework.**

**Admin Voter Login Page**

This form controls both the admin login and voter login ID. The system admin has to register the voter candidate before they can have access to the dashboard to vote for party candidate his/her choice. While in the admin login page, the admin will login with his/her username and password to the admin dashboard.



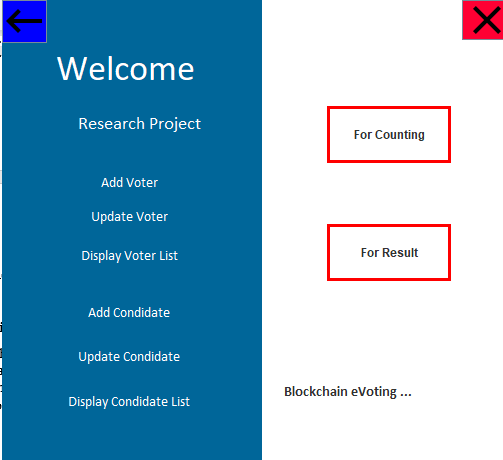
***Figure 9****: Admin Login and Voter Login*



***Figure 13:*** *Election outcome interface*

**Admin Welcome Dashboard**

This form control admin dashboard that contains the following task such as add voter, update voter, display voter list, add candidate, update candidate and display candidate list and as well display the voter counter and party candidate winner.



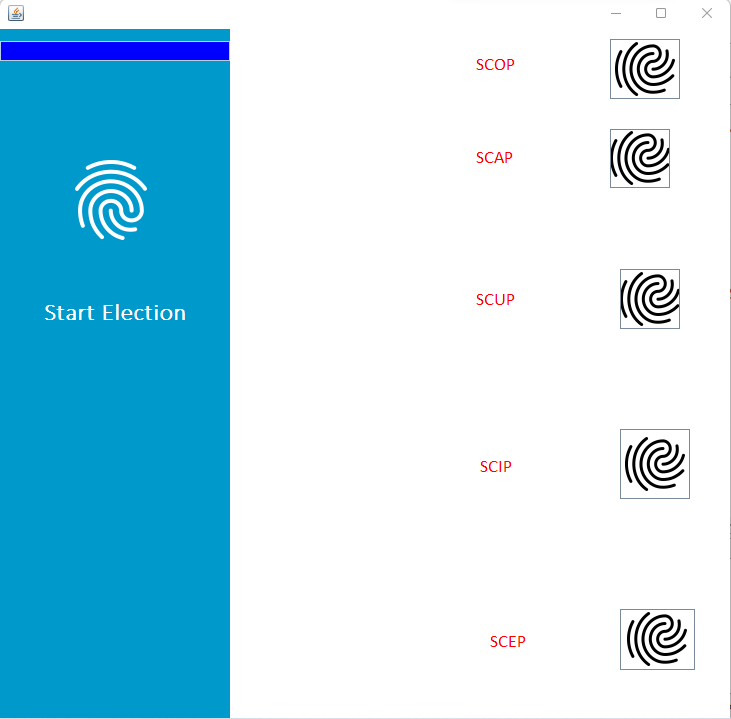
**Figure 10**: Admin Welcome Dashboard

**Add Voter Details**

This form is used to add the voter’s details, before he/she can voter for party candidate of his/her choice. It contains the input variable like voterId, Password, Name, Father Name, address etc.

Figure 11 and Figure 12 depict the screen of where voters would vote for their preferred candidate and election respectively.

***Figure 12:*** *Voting Interface*



**3.1 Blockchain Result**

In table 1, the levels of blockchain encryption are indicated where each block has different level of hash function, the output also differs for each candidate. The transaction shows that there is a level of SHA-256 algorithm embedded in the block. This also show the Proof-of-Work consensus algorithm embedded in the Ethereum blockchain technology. The Miner’s reward shows the reward of the hash function which is 30.0 bitcoin.

**Table 1:** Table 1: Blockchain Result table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/N | Blocks | Transaction | Candidate Votes | Output/Hash Function |
| 1 | 0-transaction1 | 0878634beec823b0fd1cc0456f8b5de075ccd17cb09685febd24c71065825a5c-0000000000000000000000000000000000000000000000000000000000000000 | Start Vote Candidate | 0878634beec823b0fd1cc0456f8b5de075ccd17cb09685febd24c71065825a5c |
| 2 | 1-transaction2 | 007dd03557a49352ce11c75ecf2227b54c5dca2b14dbb5b1092a9b1a8409e804-0878634beec823b0fd1cc0456f8b5de075ccd17cb09685febd24c71065825a5c | Start Vote Candidate | 007dd03557a49352ce11c75ecf2227b54c5dca2b14dbb5b1092a9b1a8409e804 |
| 3 | 2-transaction3 | 044c19395172d33aa84bc39416b7e670a6993b6ab2b803ce5ca91712640ef1ed-007dd03557a49352ce11c75ecf2227b54c5dca2b14dbb5b1092a9b1a8409e804 | Start Vote Candidate | 044c19395172d33aa84bc39416b7e670a6993b6ab2b803ce5ca91712640ef1ed |
|  | **Miner's reward: 30.0** | | | |

**4. CONCLUSION**

In this paper, we proposed a framework for e-voting systems using blockchain technology in other to improve the state of electronic voting system in Nigeria. The primary aim of adding blockchain is to increase trust in the system and to aid the security process of the application. The study highlights the faults in the paper-based method of voting as well as the limitation of a centralized voting system, this paper also illustrates the use of blockchain in other aspect of everyday livelihood and how it can be applied effectively in the electronic voting system domain. We implemented the framework designed using current technologies and we customized the system by implementing the SHA-256 encryption algorithm from ethereum where we have blocks of transactions in various stages. In future works more advanced algorithms such as AES, ECC, SHA-512 amongst others would be integrated into the system for improved data security. Other permissionless based blockchain consensus algorithm would also be integrated into the systems and their performances analysed. The System Usability Scale (SUS) would be used for empirical analysis with existing systems for comparative analysis basis and to also identify the strengths and limitations of our system with existing systems.

**REFERENCES**

Abayomi-Zannu, T. P., Odun-Ayo, I. A. & Barka, T. F. (2019). A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication, *Journal of Physics*: Conference Series, 1378, 032104

Agbu O. (2016). Election rigging and the use of technology: The Smart card reader as the Joker in Nigeria’s 2015 Presidential Election, *Journal of African Elections, 15*(2), 90-111

Ahlkvist, J., Gustafsson, A., Lundborg, C., Mattsson, J. T., Sandstedt, A., & Slavnic, S. (2019). A Decentralized Voting System. Gothenburg, Sweden: Chalmers University of Technology.

Ahmada, S., Abdullahb, S. A. J. and Arshadc, R. (2015). Issues and Challenges of Transition to e-Voting Technology in Nigeria. *Public Policy and Administration Research, 5*(4), 95-102

Al-madani, A. M., Gaikwad, A. T., Mahale, V. and Ahmed, Z. A. T. (2020) "Decentralized E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 176-180,

Ante, L. (2020). Smart Contracts on the Blockchain - A Bibliometric Analysis and Review. Blockchain Research Lab (BRL) Working Paper Series, 10, 1-48.

Antonopoulos, A. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media Inc.

Baygin, N., Baygin, M. and Karakose, M. (2019). "Blockchain Technology: Applications, Benefits and Challenges," 2019 1st International Informatics and Software Engineering Conference (UBMYK), pp. 1-5,

Bore, N, Karumba, S., Mutahi, J., Darnell, S. S., Wayua, C. & Weldemariam, K. (2017). Towards Blockchain-enabled School Information Hub Proceedings of the Ninth International Conference on Information and Communication Technologies and Development 19, ACM.

Casino, F., Dasaklis, T. K., Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics, 36*, 55-81

Christidis, K. & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things, IEEE Access, 4, 2292-2303

Dhillon, A., Kotsialou, G., McBurney, P., & Riley, L. (2020).Long Read: How blockchain can make electronic voting more secure. Retrieved from https://blogs.lse.ac.uk/usappblog/2020/09/25/long-read-how-blockchain-can-make-electronic-voting-more-secure/

Ejalonibu, G. L. (2021). Promoting Public Trust in Nigeria’s Election Administration: Explaining the Role of INEC’s Electoral Integrity. *International Journal of Scientific & Engineering Research, 12*(9), 50-68

Esteve, J. B., Goldsmith, B. and Turner, J. (2012). “International Experience with E-voting: Norwegian E-vote Project”, International Foundation for Electoral Systems, 1850 K Street, NW, Fifth Floor Washington, DC 20006, 2012

Hao, F., Kreeger, M., Randell, B., Clarke, D., Shahandashti, S., & Lee, P. (2014). Every Vote counts: Ensuring Integrity in Large-Scale Electronic Voting. 2014 Electronic Voting Technology. Workshop on Trusworthy Elections. San Diego: USENIX Association.

Hou, H. (2017). The application of blockchain technology in E-government in China. 26th International Conference on Computer Communications and Networks, ICCCN

Hoy, M. B. (2017). An introduction to the blockchain and its implications for libraries and medicine, *Med. Ref. Services Q., 36* (3) (2017), pp. 273-279

Hsiao, J. H., Tso, R., Chen, C. M., Wu, M. E. (2018). Decentralized E-Voting Systems Based on the Blockchain Technology. In: Park, J., Loia, V., Yi, G., Sung, Y. (eds) Advances in Computer Science and Ubiquitous Computing. Lecture Notes in Electrical Engineering, 474, 305-309, Springer, Singapore.

IBM. (2021). Hyperledger: Blockchain Collaboration changing the Business World. Retrieved April 30, 2022, from IBM Blockchain: https://www.ibm.com/blockchain/hyperledger.html.

Jafar, U., Aziz, M. J. A. & Shukur, Z. (2021). Blockchain for Electronic Voting System. Review and Open Research Challenges, *Sensors, 21*, 5184.

Jin, T., Zhang, X., Liu, Y., Lei, K., 2017. BlockNDN: a bitcoin blockchain decentralized system over named data networking. In: International Conference on Ubiquitous and Future Network, 75–80.

Juneja, A., Marefat, M. (2018). Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: 2018 IEEE EMBS International Conference on Biomedical and Health Informatics, 393–397.

Kennedy, Z.C., Stephenson, D.E., Christ, J.F., Pope, T.R., Arey, B.W., Barrett, C.A. & Warner, M.G. (2017). Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology, *J. Mater. Chem. C, 5* (37), 9570-9578

Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. *International Journal of Electronic Government Research, 14*(1), 53–62.

Khan, S., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain Smart Contracts: Applications, Challenges and Future Trends. *Peer-to-Peer Networking and Applications, 14*, 2901-2925.

Kucharczyk, M. (2010). Blind Signatures in Electronic Voting Systems. In: Kwiecień, A., Gaj, P., Stera, P. (eds) Computer Networks. CN 2010. *Communications in Computer and Information Science, 79*. Springer, Berlin, Heidelberg.

Malakhov, I., Marin, A., Rossi, S & Smuseva, D. (2022). On Use of Proof-of-Work in Permissioned Blockchains: Security and Fairness. *IEEE Access, 10*, 1305-1316

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *Financial Cryptography and Data Security*, 357–375.

Musa, M. A. & Aliyu, F. M. (2013). Design of Electronic Voting Systems for Reducing Election Process. *International Journal of Recent Technology and Engineering, 2*(1), 183-186

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfede, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Oke, B., Olaniyi, O., Aboaba, A., & Arulogun, O. (2019). Securing Electornic Voting System using Crystographic Technique. *ATBU Journal of Science, Technology & Education (JOSTE), 7*(1), 88-105.

Paech, P. (2017). The governance of blockchain financial networks. *Modern Law Rev., 80* (6) (2017), 1073-1110

Peng, L., Yan, W. F. Z., Li, Y., Zhou, X., Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks, 7*(3), 295-307

Pichel, F. (2016). Blockchain for land administration. *GIM Int., 30* (9), 38-39

Polge, J., Robert, J., & Le Traon, Y. (2020). Permissioned blockchain frameworks in the Industry: A comparison. *ICT Express*, 1-12.

Rawat, D. B., Choudhary, V., & Doku, R. (2020). Blockchain Technology: Emerging Applications and Use cases for Secure and Trustworthy Smart Systems. *Journal of Cybersecurity and Privacy*, 4-18.

Rivera, R., Robledo, J.G., Larios, V.M., Avalos, J.M., 2017. How digital identity on blockchain can contribute in a smart city environment. In: 2017 International Smart Cities Conference (ISC2), pp. 1–4.

Rokibul Alam, K. M. and Tamura, S. (2012). "Electronic voting - Scopes and limitations," 2012 International Conference on Informatics, Electronics & Vision (ICIEV), 2012, pp. 525-529

Rouhani, S. and Deters, R. (2021) "Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation," in IEEE Access, 9, 90379-90391

Ryan, P. (2008). Prêt à Voter with Paillier encryption. *Mathematical and Computer Modelling, 48(9–10)*, 1646–1662.

Subramanian, S., & Kamatham, S. (2019). Secure Online Election System. *International Journal of Innovative Technology and Exploring Engineering, 8*(11S), 1166-1151.

Uzedhe, G. O. and Okhaifoh, J. E. (2016). A Technological Framework for Transparent E-Voting Solution in the Nigerian Electoral System. *Nigerian Journal of Technology, 35*(3), 627-636

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 151.

Xu, R., Zhang, L., Zhao, H & Peng, Y. (2017). Design of network media’s digital rights management scheme based on blockchain technology. 13th International Symposium on Autonomous Decentralized Systems, 128-133, IEEE Proceedings

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. U.S. Department of Commerce.

Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, 137, 1-9

Ying, W., Jia, S. & Du, W. (2018). Digital enablement of blockchain: evidence from HNA group *Int. J. Inf. Manage., 39* (2018), 1-4

Yoshida, H., Biryukov, A. (2006). Analysis of a SHA-256 Variant. In: Preneel, B., Tavares, S. (eds) Selected Areas in Cryptography. SAC 2005. Lecture Notes in Computer Science, 3897. Springer, Berlin, Heidelberg.

Zhang, M., Romero, S. (2020). Design and Implementation of an e-Voting System Based on Paillier Encryption. In: Arai, K., Kapoor, S., Bhatia, R. (eds) Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, 1129. Springer, Cham.

Zhang, S. & Lee, J. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express, 6*(2), 93-97

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V. & Yalansky, L. (2017). Ensuring data integrity using blockchain technology. Conference of Open Innovation Association, FRUCT (2017), 534-539