Research Article / Review Article FUPRE JOURNAL 8(3): 121-135(2024)

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Deployment of a Secure Blockchain-based Electronic Voting for Undergraduates in Nigeria

ERHUMU, F. E. [1,*], *ALLENOTOR, D.* [2]

[1,2]*Department of Computer Science, College of Science, Federal University of Petroleum Resources Effurun, Delta State*

ARTICLE INFO

Received: 08/07/2023

Accepted: 23/04/2024

Keywords

Virtual key-card,
NodeMCU
Arduino
Raspberry Pi
Embedded systems

ABSTRACT

In Nigeria, the democratic governance relies on elections for selecting leaders, but the integrity of this process is vital for sustaining democracy. Developing democracies, like Nigeria, face challenges such as the potential for electoral violence and manipulation. The current paper-based voting system in Nigeria is susceptible to data manipulation and lacks transparency. This study proposes a Semi-Decentralized electoral system utilizing the Ethereum blockchain to enhance the security, auditability, and efficiency of the electoral process. The system aims to resist malpractices, reduce costs, and expedite the vote counting process while minimizing human intervention. The blockchain's tamper-proof nature and decentralized structure provide a secure and reliable platform for electoral data. To understand the root causes of electoral malpractice, qualitative research was conducted in Sapele Ward IV, Delta state, revealing self-interest, poverty, and a lack of trust in the government as primary motivators. The implementation of the blockchain-based electoral system demonstrated improved efficiency in collecting, collating, securing, and publishing election results. This innovative approach enhances the perceived integrity of the electoral process, addressing key challenges in the current voting system.

1. INTRODUCTION

Elections and voting are the fundamental notions in the modern democratic landscape, as they both represent the core and focal point in civic engagement and governance thereof. Elections are the means by which people as a group convey their preferences for choosing a representatives or reaching critical decision (Abuidris et al., 2019). The blockchain is fast developing as a transformational instrument. Its introduction as a new tech has improved the security and integrity of these procedures (Aghware et al., 2023b, 2023a; Akazue et al., 2023; Ojugo, Akazue, et al., 2023; Ojugo, Ejeh, et al., 2023). Although, the blockchain was first proposed as a fundamental tech to serve as cryptocurrencies – its usage and the consequent adoption in other fields other than its use as money has become imperative and critical (De' et al., 2020; Fan et al., 2022; Lei et al., 2022; Quamara & Singh, 2023) – and to include in election processes to ensure notable elections . In order to establish the foundation for a more thorough examination of the relations between elections, voting, and blockchain technology, and change the nature of democratic practices (Damoska & Erceg, 2022; Nguyen et al., 2021; Ojugo, Odiakaose, et al., 2023; Sedlmeir et al., 2020).

An election is a formal process where

*Corresponding author, e-mail: erhumufelix@gmail.com

persons or groups make choices or decisions by voting (Omran Aly, 2014). Elections are used to select representatives and/or leaders who make decisions on specific issues within a community, or political entity (Okuyama et al., 2014; Ometov et al., 2021). The voting process allows eligible participants to express their preferences, and the candidate or option with the most votes usually emerge as a winner. Callen (2016) described election as the process by which the populace selects its leaders, expresses their preferences for policies and programs, and, as a result, grants a government the power to rule (Callen et al., 2016).

1.1 The Electoral System

How a people select a candidate of their choice to a place of authority – is described as election. The regulations that govern how elections and votes are held and how their outcomes are determined is known as an electoral system or voting system. All aspects of the voting procedure are governed by these laws, including when and where elections take place, who is eligible to vote (Ojugo et al., 2012; Ojugo, Ejeh, et al., 2023) who may run for office, how ballots are labelled and cast, how they are counted, how the results of the vote are determined, spending caps on campaigns, and other elements that may have an impact on the outcome (Mamun et al., 2022; Mao et al., 2018; Murthy et al., 2020; Ojugo & Eboka, 2019b). The constitutions and electoral laws define political electoral systems, which are normally run by election commissioners and are capable of using a variety of elections for various offices. This procedure establishes as well as specifies the standards that must be satisfied by a party or candidate in order to run for office and how votes are counted (Yoro, Aghware, Akazue, et al., 2023; Yoro, Aghware, Malasowe, et al., 2023).

Reynolds (2005) An electoral system is designed to impact all aspects of its electoral laws. The choice of electoral system has an influence on the way boundaries are drawn, how voters are registered, the design of ballot papers, how votes are counted, and numerous other aspects of the electoral process. There are numerous election systems in use today, with numerous variations on each. They can be divided into three main families: mixed systems, proportional representation systems, and plurality/majority systems. Nigeria uses a Plurality/ majority electoral system called First Past The Post (FPTP).

Elections continue to be the most suitable and widely used method for choosing the people's representatives, who will be in charge of governing on their behalf (Hounkpe, Gueye, & Badara, 2010). The integrity of the electoral process is crucial to the integrity of democracy (Annan, et al., 2012). A country's electoral process must be clear and understandable enough for voters and candidates to accept the outcomes. Unfortunately, Elections in developing democracies and post-war cultures carry a significant risk of reigniting violent conflict, undermining stabilization efforts, and undermining democratization. It has been transformed from a tool of democratic participation but also a fierce contest for positions of leadership, power and access to resources (winrich, 2010).

Electoral malpractices on the Nigerian front from eyewitness reports to new sources includes result falsification by security, ad-hoc recruited staffs etc, multiple voting by voters using the same card, under-aged voting, use of illegally acquired voting cards to vote on election days, concealment or non-release of voters' register loaded with false names, voters register used at polling units not numbered, thus permitting arbitrary addition of names to the register, missing names of some registered voters, intimidation and disfranchisement of voters, snatching or destruction of ballot boxes, miscomputation and falsification of result by staffs, increasing the number of invalid votes to reconcile the total number of votes on the card reader, not using card reader so as to enable the manipulation of accredit voters as they see fit, and using spirit to

clean the indelible ink.
Others committed by the upper level of administration includes to influence results in favour of the incumbent party or rulers, the diversion of electoral materials to enable the falsification and other forms of manipulation, changing of electoral staff few days to election day etc. One can deduce from this – that Nigeria has performed poorly in all her elections; And this, has since been identified as the greatest menace and threat to this nation's democracy.

1.2. The Blockchain Technology

Blockchain is a complex data structure in which growing records are stored in blocks. Its 4-basic elements are data, current block hash, previous block hash, and timestamp. So, if we add new data blocks to the blockchain, each new block is linked to the previous one. using a hash value which makes it immutable, and all the workflow is recorded are time-stamped which places an identity to it and the replicas are distributed to each network node that is a participant, this guarantees that the data integrity is kept between the endpoints without any human involvement (Naz & Lee, 2020; Nazir et al., 2017; Nishi et al., 2022).
A blockchain is a distributed transaction ledger (Onik et al., 2019). It is a distributed database in which a linear collection of data elements called blocks are linked together to form a chain, and secured by cryptographic primitive (Ojugo et al., 2021b, 2021a). It is a record-keeping mode that uses decentralised distributed database. The list of records is kept in a block, which is linked together to form a chain. Hacking a blockchain is tough because if one block is hacked, the attacker must hack every block because each block's hash pointer is linked to the next (Omar et al., 2020; Ometov et al., 2021). First, blocks are provably immutable. This is possible because each block contains a hash, or numeric digest of its content, that can be used to verify the integrity of the containing transactions. Next, the hash of a block is dependent on the hash of the block before it. This effectively makes the entire blockchain history immutable, as changing the hash of any block (Ojugo et al., 2013; Okuyama et al., 2014; Omar et al., 2021).

1.3. Electronic Voting and Data Integrity

Annan, et al., (2012) defines election integrity as any election that is conducted in a professional, unbiased, and transparent manner throughout the whole electoral cycle and is founded on the democratic values of universal suffrage and political equality as reflected in international norms and agreements. It is dangerous to take electoral integrity for granted. Within the official body of election administration, mechanisms for promoting and upholding integrity in every step of the electoral process are frequently implemented. These mechanisms allow for monitoring of electoral administration operations, oversight of the electoral process by other governmental sectors or agencies, civil society, and the media, and provision for the judicial or administrative enforcement of electoral laws and regulations. Without electoral integrity, there is little public trust in the election results, leaders and officials are not held accountable, and the government lacks essential legitimacy. Public trust in political and electoral systems is a requirement for election integrity. Political structure reform is not sufficient; the public must be persuaded that the changes are genuine and deserving of their trust. Building such confidence requires among other things inclusivity, transparency, and responsibility.

(DANILLER & MUTZ, 2019) study was aimed at investigating the impact of democratic outcomes on individuals' perceptions of electoral integrity, particularly in the context of American presidential elections. He aimed at exploring whether positive reactions to winning and negative reactions to losing balance each other out, thereby maintaining a relatively constant perception of electoral integrity in a highly competitive political

environment like the United States. The research employs panel data covering over nine years, spanning three American presidential election cycles. The study's main conclusions imply that winning and losing have different effects. Put differently, different people's opinions of electoral integrity are affected differently by these outcomes. The study also shows that these effects on people's perceptions are remarkably long-lasting. In particular, voters' perceptions of the democratic process are significantly and permanently altered by recurrent electoral defeats.

In another study conducted by (Garnett & James, 2020), the authors present a new method of assessing the integrity of elections by emphasizing the importance of practitioner knowledge. They assert that electoral officials possess unique, practice-based, experiential, and tacit knowledge about the conduct of elections, which is not fully captured by public and expert perceptions. This practitioner knowledge includes insights into the technical aspects of administration that may not be apparent to the public or even to other experts. To support their case, the author presents results from the first-ever cross-national datasets derived from a survey of electoral officials in 31 countries. These practitioner assessments of electoral integrity are then compared to assessments from experts and the public – traditional methods of evaluating electoral integrity (Ojugo & Otakore, 2018a, 2018b). The findings indicate that practitioner assessments are a reliable measure of electoral integrity, suggesting that the unique insights of electoral officials should be considered when evaluating the fairness and integrity of elections. Furthermore, he discussed how gender and job satisfaction can influence practitioner assessments. The analysis suggests that certain electoral malpractices might have gendered aspects, and job satisfaction is a significant factor that should be taken into account in future studies.

(Norris, Frank, & Coma, 2014) research design involves a survey-based approach using a set of indicators and an overall index to evaluate the perceived quality of elections. The primary objective was to determine the validity of claims regarding fraud, irregularities, and malpractices in contentious elections. Survey of election experts were carried out providing valuable insights into the electoral processes (Suleiman & Reza, 2019). The survey comprises 49 indicators that were clustered into 11 stages of the electoral cycle. This approach allows for a comprehensive evaluation of the entire election process (Braddock & Chambers, 2011). The study compares the quality of elections globally using the Perception of Electoral Integrity (PEI) 100-point index dataset generated from the survey. This index serves as a quantitative measure to gauge the perceived quality of elections. It condenses the complex evaluation into a numerical score (Nassar & Al-Hajri, 2013). This dataset is a new addition to evidence available to assess problems of electoral integrity. The study claims high levels of external and internal validity, suggesting that the findings are applicable beyond the specific cases studied.

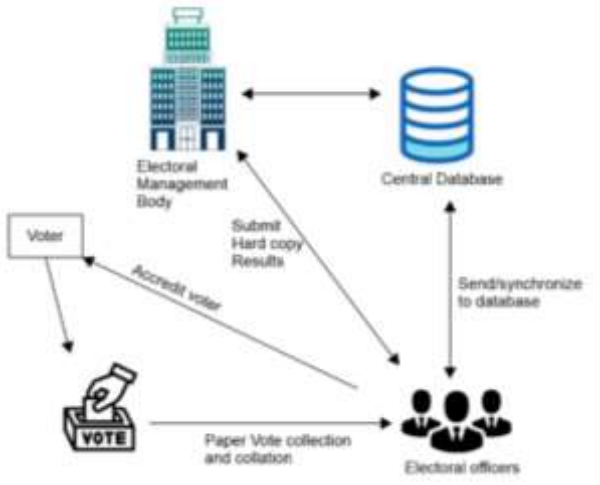

Figure 1. Existing System design (Okonta et al., 2013, 2014; Wemembu et al., 2014)

The study is motivated (Ojugo, Eboka, et al., 2015a, 2015b) as thus:

1. The unwillingness of stakeholders to disclose accurate data in the course of electioneering and during the collation

of results – has led to the unavailability of data for extensive study. To combat this – we use a hyper-ledger fabric framework.
2. Previous studies used a centralized model, which has not improved transparency, user-trust, and transaction security that is required to ensure credible elections.
3. With no controldue to external/internal influences of the election process, the quality of the election become erratic and marred with all forms of violence, corruption etc.

Our study seeks to explore a block-chain-based electronic voting system.

2. MATERIALS AND METHODS

2.1. Proposed Electronic Medical Records Blockchain Ensemble

We employ a 3-tier framework to model our blockchain for voting data exchange. The blockchain creates a secure, transparent space for the electronic records and serves as its hidden focal database to aid authentication of exchanged data, security and storage (Chaieb et al., 2019; S. K. Singh et al., 2020). The chain-codes consist a 3-tier n-client that aids effective transfer of voting records via the blockchain. The logic layer processes data by interfacing with the hash-codes in each blockchain to ensure data integrity (Wang et al., 2020). Each hash-code is generated via the hyper-ledger fabric which maps an input of varying length (i.e., voter's data) to a hashed output of fixed length. This hashed output value of the record is then morphed when the block of data for the electoral record changes. The nodes on the blockchain then inspects and validates any new voter's record as either a store or retrieve transaction request. Each request is filed via a distributed consensus by a variety of validating nodes (as no single node on a chain validates or has central control of the network) – making it tedious for voter data and election results records to be altered, distorted, corrupted, compromised and/or stolen (Abakarim et al., 2018; Abbasi et al., 2016; Albladi & Weir, 2018; Allenotor et al., 2015; Allenotor & Ojugo, 2017).

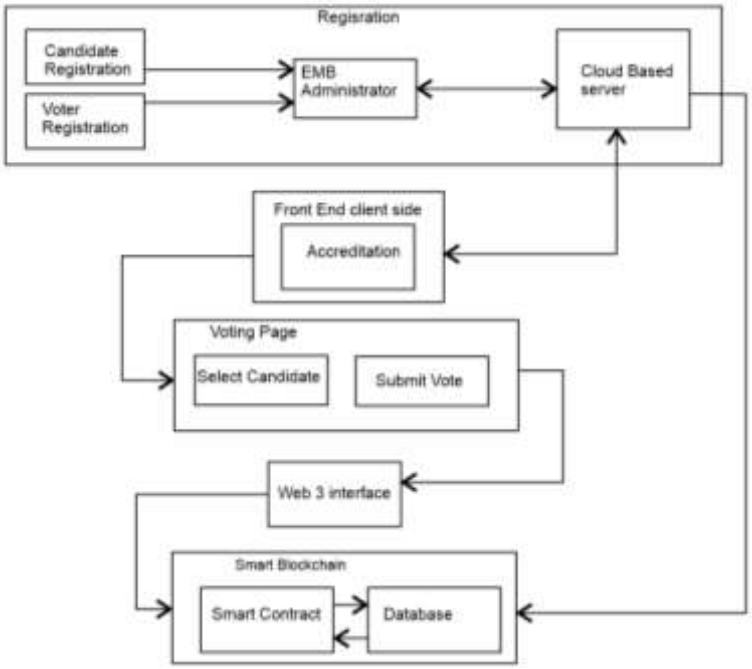

Figure 2. Block diagram of the proposed system

The user-interface helps to effectively manage data access, server-side procedures, and storage; while, keeping each as an autonomous segment on isolated stages

using n-fat client framework (K. W. Brown & Armstrong, 2023; W. Brown & Armstrong, 2015). Our 3-tier design allow each layer to be redesigned or supplanted freely without system downtime. Our design architecture is thus inspired by (A. Singh et al., 2020; Stanisławek et al., 2021) to consists of: (a) the client module – identifies data with allowed, accessible services on the mobile app, which enables a user interact with other layers in the system by sending user query results via a P2P network, (b) the application server yields the business logic of the blockchain (Ojugo & Eboka, 2021), which controls the application and yields the smart contracts using the hyper-fabric ledger, and (c) the blockchain database houses the business logic – acting as a database server for data storage and recovery (Alakbarov & Hashimov, 2018; Datta et al., 2021; Joshi et al., 2021; Ojugo & Yoro, 2020b; Pradeepa & Parveen, 2020).

2.2. Proposed Structure and Chaincodes

The chain-code(s) as in figure 2 details transition of records between actors (i.e. voter, practitioner, database), and how medical records are distributed and changes their state from one stakeholder to another. These transactions use the smart-contracts logic to execute and regulate these transitions, and yields traceability, transparency and efficiency of these records as they move between these unique states (Ojugo & Yoro, 2021b). The records and states are stored in the hyper-fabric ledger. Details of the chain-code structure is as thus (Despoudi et al., 2021; Wright & De Filippi, 2015).

1. *Stage 1: Ledger State* – The medical record represents a set of properties with assigned values that creates a unique keyset as well as the state of the voter record. The voter_list is the complete keyset, with its state initialized as a record in the world state on the hyper-fabric ledger. This record supports several states with attributes that allows the same ledger in its world-state to hold various records of the same voter. This makes possible the capability of the system to evolve and update its state(s) and structure.
2. *Stage 2: Proof-of-Trust* – With a variety of roles (not limited to the) commission personnel, adhoc staff and the electorates, we have a variety of transaction(s) etched in the smart contract with enshrined rules for: (a) transition of records between the actors, (b) how different business interests must approve a transaction, and (c) how each individual state keys work. It implies that the chain must set a rule in the namespace to define a business logic or transaction that processes a specific voter_record, and set another to update all retrieved/processed record assets to portray trust relations of the transactions.
3. *Stage 3: Smart Contract* – Here, a smart-contracts code set all valid states for a voter record and the logic that transitions it from a state to another. Smart contract sets up key-business processes and information to be shared across various actors interacting on the network. It defines the various states of a business manages the various processes to move an asset/record between these states. In the network, the same smart contract is shared and used by the different nodes and by the different applications connected therein. Thus, it jointly executes a shared business data and process. All members of the network must agree a specific version of smart contract to be used.

2.3. The Activity Diagram

An activity diagram represents a series of actions or flow of control in a system similar to flowchart or a data flow diagram. The activities modelled can be sequential and concurrent (Chevalier et al., 2003; Tarafdar & Zhang, 2005). Figure 3 shows the activities performed by each entity/class of the system and these activities are discussed thus:

1. The election personnel and voter attempt to login by entering their respective usernames and passwords, and await authorization from the blockchain database. If the username and password is invalid it aborts the operation but if valid the users (election personnel and voter) gains access into the system and are assigned individual privileges.
2. The election personnel views voters' medical history, diagnose, run tests on the voter and then upload the medical results into the system. The blockchain encrypts the medical result and shares to multiple participants in the network for consensus (Ibor et al., 2023; Ojugo & Nwankwo, 2021; Ojugo & Yoro, 2021a).
3. The voter views the uploaded results by the commission and can also request for modification in biodata. The request is sent to the blockchain database and propagated across the network for subsequent approval or decline of the request. If the request is approved the changes are effected otherwise the operation is aborted. One participant cannot make changes without the consensus of other participants in the network, otherwise the data is said to be compromised. (Ojugo & Yoro, 2020a, 2020c).

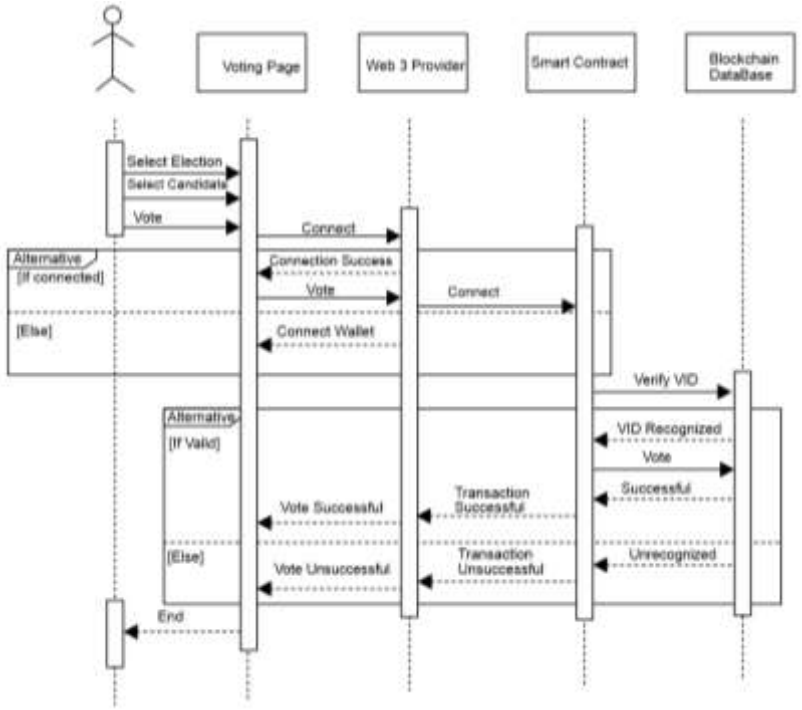

Figure 3. System flowchart of the proposed system

3. RESULT FINDINGS AND DISCUSSION

3.1. Response Time

This performance metric seeks the time interval between a user's request and actual time a response is fed back as in figures 4.

Figure 4. Response time with 2500-users

Response time for our database queries was about 0.38secs, for email download 0.008secs, 0.052secs for file download and 0.32secs for page retrieval There is no significant difference in response time for the applications. We conclude that the response time even with when doubled is still scalable. Table 1 is a vivid picture of the simulation results for electronic voting system app used by undergraduates in Federal University of Petroleum Resources Effurun.

Table 1. Scalability Result

Items	Scenario 1	Scenario 2	Scenario 1	Scenario 2
	Time Secs	Population	Time Secs	Population
DB Query	0.38	0.40	3512	7230
Email	0.008	0.015	3512	7230
FTP	0.052	0.060	3512	7230
HTTP	0.32	0.35	3512	7230

3.2. Application Throughput

Throughput is the actual transfer rate of data in a medium over given a period of time. It checks capacity of a network data transfer rate as analyzed in Figure 5.

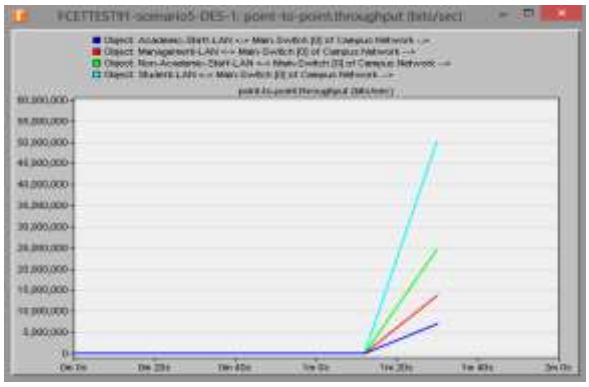

Figure 5: Throughput test

The highest data transfer rate was about 47.68mbps, which agrees with (Cerf, 2020; Charan et al., 2020; Manickam et al., 2022). We clearly see that different nodes were sent echo request, and an eighty per cent (80%) response rate was gotten. This was solely because it was the first time. Subsequent echo request had a success rate of a hundred per cent. This clearly shows that the different nodes were reachable (Ojugo, Allenotor, et al., 2015; Ojugo & Eboka, 2019a; Yoro & Ojugo, 2019).

3.3. Discussion of Findings

While the adoption of blockchain in electoral systems has proven successful in various aspects, it is essential to address challenges such as scalability, accessibility, and regulatory considerations. Nevertheless, the positive outcomes observed so far suggest that blockchain holds great promise in revolutionizing electoral processes by creating a more secure, transparent, and efficient foundation for democratic practices.

Phishing and social engineering threats are effectively countered through a multi-faceted approach (Ojugo & Eboka, 2014, 2018). User education plays crucial role in empowering individuals to recognize and resist deceptive tactics. Also, implementation of two-factor authentication (2FA) for remote access and voting adds an extra layer of security, requiring additional verification beyond passwords (Ojugo & Ekurume, 2021). Clear and prominent warnings further enhance user awareness, alerting them to potential risks and encouraging cautious online behaviours. A comprehensive strategy is collectively required to strengthens the electoral system defences against socially-engineered attacks, mitigating the associated cybersecurity risks (Jáñez-Martino et al., 2022; Kumaraguru et al., 2010; Sahmoud & Mikki, 2022).

Also, transition from traditional election method cum process to blockchain electronic voting presents logistical hurdles, including the need for widespread technological adoption, addressing potential resistance from stakeholders, and ensuring accessibility for all demographics. To navigate these, a phased approach is recommended, starting with pilot programs to showcase the benefits and reliability of blockchain voting. Also, a comprehensive

public education campaigns and collaboration with key stakeholders can help build trust in the new system, fostering a smoother transition. Continuous monitoring and adaptation based on feedback will be essential to refine the blockchain voting method and address emerging challenges.

4. CONCLUSION

Based on these, the study recommends: (a) the electoral commission needs to act quickly to inform the people about the voting process, political rights, and risks associated with electoral fraud, (b) the executive should stay not partake in the appointment of the electoral commission's chairman as this upsets the balance of power and this new chairman will be influenced in the discharge of his/her duties, (c) stricter penalties should be meted for electoral fraud to discourage election defaulters, (d) explore a blockchain, decentralized approach to manage electoral data, (e) minimize human intervention in the collation process, and (f) outlaw the norm of political godfatherism and political puppets.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Abakarim, Y., Lahby, M., & Attioui, A. (2018). An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications*, 1–7. https://doi.org/10.1145/3289402.3289530

Abbasi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 169–174. https://doi.org/10.1109/ISI.2016.7745462

Abuidris, Y., Kumar, R., & Wenyong, W. (2019). A Survey of Blockchain Based on E-voting Systems. *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, 99–104. https://doi.org/10.1145/3376044.3376060

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. https://doi.org/10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment analysis in detecting sophistication and degradation cues in malicious web contents. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 653.

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Alakbarov, R., & Hashimov, M. (2018). Application and Security Issues of Internet of Things in Oil-Gas Industry. *International Journal of Education and Management Engineering*, *8*(6), 24–36. https://doi.org/10.5815/ijeme.2018.06.03

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*,

8(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal*, *3*(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. *African Journal of Computing & ICT*, *8*(2), 83–92. www.ajocict.net

Braddock, R., & Chambers, C. (2011). Tank gauging systems used for bulk storage of gasoline. *Institution of Chemical Engineers Symposium Series*, *156*, 553–559.

Brown, K. W., & Armstrong, T. J. (2023). Hydrocarbon Inhalation. In *StatPearls*. http://www.ncbi.nlm.nih.gov/pubmed/24911841

Brown, W., & Armstrong, T. J. (2015). *Personnel Protection and Safety Equipment for the Oil and Gas Industries*. Elsevier. https://doi.org/10.1016/C2014-0-03648-9

Callen, M., Gibson, C. C., Jung, D. F., & Long, J. D. (2016). Improving Electoral Integrity with Information and Communications Technology. *Journal of Experimental Political Science*, *3*(1), 4–17. https://doi.org/10.1017/XPS.2015.14

Cerf, V. G. (2020). On the internet of medical things. *Communications of the ACM*, *63*(8), 5–5. https://doi.org/10.1145/3406779

Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). *Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol* (pp. 16–30). https://doi.org/10.1007/978-3-030-11395-7_2

Charan, D. S., Nadipineni, H., Sahayam, S., & Jayaraman, U. (2020). *Method to Classify Skin Lesions using Dermoscopic images*. http://arxiv.org/abs/2008.09418

Chevalier, K., Bothorel, C., & Corruble, V. (2003). Discovering Rich Navigation Patterns on a Web Site. In *Webometrics* (Vol. 5, Issue 6, pp. 62–75). https://doi.org/10.1007/978-3-540-39644-4_7

Damoska, S. J., & Erceg, A. (2022). Blockchain Technology toward Creating a Smart Local Food Supply Chain. *Computers*, *11*(6), 95. https://doi.org/10.3390/computers11060095

Datta, S. K., Shaikh, M. A., Srihari, S. N., & Gao, M. (2021). *Soft-Attention Improves Skin Cancer Classification Performance*. http://arxiv.org/abs/2105.03358

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*(June), 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Despoudi, S., Papaioannou, G., & Dani, S. (2021). Producers Responding to Environmental Turbulence in the Greek Agricultural Supply Chain: Does Buyer Type Matter? *Knowledge: Toward a Media History of Documents*, *3*(April), 49–58.

Fan, Z.-P., Wu, X.-Y., & Cao, B.-B. (2022). Considering the traceability awareness of consumers: should the supply chain adopt the blockchain technology? *Annals of Operations Research*, *309*(2), 837–860. https://doi.org/10.1007/s10479-020-03729-y

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(992), 1–8. https://doi.org/10.46481/jnsps.2022.992

Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo, E., & Alegre, E. (2022). A review of spam email detection: analysis of spammer strategies and the dataset shift problem. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-022-10195-4

Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31. https://doi.org/10.1145/1754393.1754396

Lei, M., Xu, L., Liu, T., Liu, S., & Sun, C. (2022). Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges. *Foods*, *11*(15), 1–31. https://doi.org/10.3390/foods11152262

Mamun, A. Al, Azam, S., & Gritti, C. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. *IEEE Access*, *10*, 5768–5789. https://doi.org/10.1109/ACCESS.2022.3141079

Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare. *Biosensors*, *12*(8). https://doi.org/10.3390/bios12080562

Mao, D., Wang, F., Hao, Z., & Li, H. (2018). Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain. *International Journal of Environmental Research and Public Health*, *15*(8), 1627. https://doi.org/10.3390/ijerph15081627

Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, *8*, 205190–205205. https://doi.org/10.1109/ACCESS.2020.3036812

Nassar, R. H., & Al-Hajri, A. R. (2013, March 10). Field Experience with Still Pipes Installation and Supporting in KOC Storage Tanks. *All Days*. https://doi.org/10.2118/164155-MS

Naz, S., & Lee, S. U.-J. (2020). Why the new consensus mechanism is needed in blockchain technology? *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 92–99. https://doi.org/10.1109/BCCA50787.2020.9274461

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

Nguyen, D. C., Ding, M., Pham, Q.-V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet of Things Journal*, *8*(16), 12806–12825. https://doi.org/10.1109/JIOT.2021.3072611

Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., & Saini, D. K. (2022). Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. *Journal of Sensors*, *2022*, 1–22. https://doi.org/10.1155/2022/7299185

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10. www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. *African Journal of Computing & ICT*, *7*(3). www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2018). Comparative Evaluation for High Intelligent Performance Adaptive Model for Spam Phishing Detection. *Digital Technologies*, *3*(1), 9–15. https://doi.org/10.12691/dt-3-1-2

Ojugo, A. A., & Eboka, A. O. (2019a). Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., & Eboka, A. O. (2019b). Signature-based malware detection using approximate Boyer Moore string matching algorithm. *International Journal of Mathematical Sciences and Computing*, *5*(3), 49–62. https://doi.org/10.5815/ijmsc.2019.03.05

Ojugo, A. A., & Eboka, A. O. (2021). Modeling Behavioural Evolution as Social Predictor for the Coronavirus Contagion and Immunization in Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(2), 135–144. https://doi.org/10.35877/454RI.asci130

Ojugo, A. A., Eboka, A. O., Okonta, E. O., Yoro, R. E., & Aghware, F. O. (2012). Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS). *Journal of Emerging Trends In Computing Information Systems*, *3*(8), 1182–1194. http://www.cisjournal.org

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015a). Framework design for statistical fraud detection. *Mathematics and Computers in Science and Engineering Series*, *50*, 176–182.

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015b). Hybrid Model for Early Diabetes Diagnosis. *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, *50*, 55–65. https://doi.org/10.1109/MCSI.2015.35

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2023). Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework. *International Journal of Informatics and Communication Technology*, *12*(3), 205. https://doi.org/10.11591/ijict.v12i3.pp205-213

Ojugo, A. A., & Ekurume, E. O. (2021). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. *International Journal of Education and Management Engineering*, *11*(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., & Nwankwo, O. (2021). Spectral-Cluster Solution For Credit-

Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network. *JINAV: Journal of Information and Visualization*, *2*(1), 15–24. https://doi.org/10.35877/454RI.jinav274

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021a). Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria. *ARRUS Journal of Mathematics and Applied Science*, *1*(2), 110–120. https://doi.org/10.35877/mathscience614

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021b). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. *ARRUS Journal of Engineering and Technology*, *2*(1), 12–23. https://doi.org/10.35877/jetech613

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Adigwe, W., Anazia, K. E., & Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., & Otakore, D. O. (2018a). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2018b). Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria. *Journal of Computer Sciences and Applications*, *6*(2), 82–90. https://doi.org/10.12691/jcsa-6-2-5

Ojugo, A. A., & Yoro, R. E. (2020a). Empirical Solution For An Optimized Machine Learning Framework For Anomaly-Based Network Intrusion Detection. *Technology Report of Kansai University*, *62*(08), 6353–6364.

Ojugo, A. A., & Yoro, R. E. (2020b). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), 5933–5947.

Ojugo, A. A., & Yoro, R. E. (2020c). Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados. *Quantitative Economics and Management Studies*, *1*(4), 237–248. https://doi.org/10.35877/454ri.qems139

Ojugo, A. A., & Yoro, R. E. (2021a). Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(3), 1673. https://doi.org/10.11591/ijeecs.v21.i3.pp1673-1682

Ojugo, A. A., & Yoro, R. E. (2021b). Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack. *International Journal of Electrical and Computer Engineering*, *11*(2), 1498–1509. https://doi.org/10.11591/ijece.v11i2.pp1498-1509

Ojugo, A. A., Yoro, R. E., Okonta, E. O., & Eboka, A. O. (2013). A Hybrid Artificial Neural Network Gravitational Search Algorithm for Rainfall Runoffs Modeling and Simulation in Hydrology. *Progress in Intelligent Computing and Applications*, *2*(1), 22–34. https://doi.org/10.4156/pica.vol2.issu

e1.2

Okonta, E. O., Ojugo, A. A., Wemembu, U. R., & Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. *West African Journal of Industrial & Academic Research*, *6*(1), 50–64.

Okonta, E. O., Wemembu, U. R., Ojugo, A. A., & Ajani, D. (2014). Deploying Java Platform to Design A Framework of Protective Shield for Anti–Reversing Engineering. *West African Journal of Industrial & Academic Research*, *10*(1), 50–64.

Okuyama, S., Tsuruoka, S., Kawanaka, H., & Takase, H. (2014). Interactive Learning Support User Interface for Lecture Scenes Indexed with Extracted Keyword from Blackboard. *Australian Journal of Basic and Applied Sciences*, *8*(4), 319–324.

Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access*, *9*, 37397–37409. https://doi.org/10.1109/ACCESS.2021.3062471

Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*(1), 224. https://doi.org/10.1186/s12874-020-01109-5

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., Chukhno, O., Ali, A., Channa, A., Svertoka, E., Qaim, W. Bin, Casanova-Marqués, R., Holcer, S., Torres-Sospedra, J., Casteleyn, S., Ruggeri, G., … Lohan, E. S. (2021). A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks*, *193*, 108074. https://doi.org/10.1016/j.comnet.2021.108074

Omran Aly, W. (2014). Bad Governance and Failure of Development Progress in Egypt Causes, Consequences and Remedies. *Journal of Public Administration and Governance*, *3*(4), 39. https://doi.org/10.5296/jpag.v3i4.4340

Onik, M. M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019). Blockchain in Healthcare: Challenges and Solutions. In *Big Data Analytics for Intelligent Healthcare Management* (pp. 197–226). Elsevier. https://doi.org/10.1016/B978-0-12-818146-1.00008-8

Pradeepa, K., & Parveen, M. (2020). Solid State Technology 8060 A Survey on Routing Protocols With Security in Internet of Things A Survey on Routing Protocols With Security in Internet of Things. *International Virtual Conference on Emerging Trends in Computing (IVCET)*, *63*(4), 38–111.

Quamara, S., & Singh, A. K. (2023). An In-depth Security and Performance Investigation in Hyperledger Fabric-configured Distributed Computing Systems. *Blockchain Models*, *1*(1), 12–24.

Sahmoud, T., & Mikki, D. M. (2022). *Spam Detection Using BERT*. https://doi.org/10.48550/arXiv.2206.02443

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, *62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Singh, A., Jadhav, S., & Roopashree, M. (2020). Factors to overcoming barriers affecting electronic medical record

usage by physicians. *Indian Journal of Community Medicine*, *45*(2), 168. https://doi.org/10.4103/ijcm.IJCM_478_19

Singh, S. K., Rathore, S., & Park, J. H. (2020). BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Generation Computer Systems*, *110*, 721–743. https://doi.org/10.1016/j.future.2019.09.002

Stanisławek, M., Miarka, D., Kowalska, H., & Kowalska, J. (2021). Traceability to ensure food safety and consumer protection as typified by case studies of three meat processing plants. *South African Journal of Animal Sciences*, *51*(2), 241–249. https://doi.org/10.4314/sajas.v51i2.12

Suleiman, R. F. R., & Reza, F. Q. M. I. (2019). Gas station fuel storage tank monitoring system using internet of things. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.6 Special Issue), 531–535. https://doi.org/10.30534/ijatcse/2019/7881.62019

Tarafdar, M., & Zhang, J. (2005). Analyzing the influence of Web site design parameters on Web site usability. *Information Resources Management Journal*, *18*(4), 62–80. https://doi.org/10.4018/irmj.2005100104

Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., & Susilo, W. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, *519*, 348–362. https://doi.org/10.1016/j.ins.2020.01.051

Wemembu, U. R., Okonta, E. O., Ojugo, A. A., & Okonta, I. L. (2014). A Framework for Effective Software Monitoring in Project Management. *West African Journal of Industrial and Academic Research*, *10*(1), 102–115. http://www.ajol.info/index.php/wajiar/article/view/105798

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2580664

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1922. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E., & Ojugo, A. A. (2019). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1