2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018)
Federal University of Technology, Minna, Nigeria
September 5 – 6, 2018

Blockchain 3.0: Towards a Secure Ballotcoin Democracy through a Digitized Public Ledger in Developing Countries

E. M. Dogo[1], N. I. Nwulu[2], O. M. Olaniyi[3], C. O. Aigbavboa[4], and T. Nkonyana[5]
[1, 2, 5]Department of Electrical and Electronics Engineering Science, University of Johannesburg, South Africa
[4]Department of Construction Management and Quantity Survey, University of Johannesburg, South Africa
[1, 3]Department of Computer Engineering, Federal University of Technology Minna, Nigeria
[1]eustaced@uj.ac.za, [2]nnwulu@uj.ac.za, [3]mikail.olaniyi@futminna.edu.ng, [4]caigbavboa@uj.ac.za, [5]tnnkonyana@uj.ac.za

***Abstract*—This paper reviews scholarly articles on the application of blockchain technology for secure electronic voting (e-voting). Furthermore, the feasibility of using blockchain technology to replace the existing manual or semi-digitized voting system in developing countries with Nigeria as a case study is performed. To analyse the current state and preparedness of adopting Blockchain Enabled E-voting (BEEV) system in Nigeria, this paper employs the qualitative SWOT (*S*trengths, *W*eaknesses, *O*pportunities and *T*hreats) and PEST (*P*olitical, *E*conomic, *S*ocial and *T*echnological) analysis approach. This evaluation leads us to identify internal and external factors and the strategic direction in adopting BEEV in Nigeria. It is the authors' opinion that this approach could also be tailored to evaluate situations of other developing countries.**

Keywords-security; E-voting; I-voting; Blockchain; Developing countries

I. INTRODUCTION

"It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything" – Joseph Stalin

Democracy is the pillar of every political system and ensures an equal and fair voting system by guaranteeing the right of all eligible voters to freely vote for their preferred party or candidate. The concern on every voters' mind is whether their vote will count and if the votes recording and the final result is accurate. Despite the tremendous technological advancement and digitization of numerous spheres of modern life, most elections are still conducted using paper-ballot and usually offline, especially in developing democracies around the world. Traditional ballot-based voting have the following inherent flaws [1-3]:

- Paper ballot prone to fraud
- Manual counting errors
- Compromise during the distribution of election materials from central locations to voting centres
- Possible compromise and interference by external companies or contractors handling the manufacture of election materials or voting database management.
- High cost associated with conducting elections
- Time-consuming
- Complex processes`

Due to the complexity, cost and time associated with conducting free, fair and credible elections, and the accusations and counter-accusations that follow every election cycle, attention is moving towards adopting current technological advances, away from the traditional paper-ballot voting system. This is in order to eliminate human errors, fraud, and biases, thereby improving trust in the electioneering processes. Consequently, over the years, scholars and democratic experts have advocated for an e-voting [4, 5] to address issues inherent in traditional ballot-paper based voting earlier outlined. This will improve voters' turnout and trust in elections by directly using electronic devices on the internet or voting software application to improve the overall democratic processes. However, the central concern in adopting an electronic voting (e-voting) system is security.

Security challenges in e-voting are well articulated in numerous literature such as [3, 6-8] and drawbacks of public key cryptographic implementations in e-voting systems [1]. Drawbacks such as computational power needed to decrypt votes, possible hacking through random number generation, and system complexities. Therefore, security remains the major concern since voting is done through the internet or dedicated network online [9] as well as trust in a central body to manage elections. Security requirement of electronic voting includes eligibility, coercion freeness, availability, anonymity, integrity, correctness/accuracy, robustness, fairness, receipt-freeness, voter verifiability and universal verifiability [1, 10].

Trust and privacy are the key elements a voter demands during an election. Trust that the voter's vote will count and privacy that the voter's choice remains personal. Centralization of the internet and cloud computing platforms is another concern since data is residing in a central location and vulnerable to cybersecurity attacks [11]. Attention is therefore shifting to blockchain Distributed Ledger Technology (DLT) as a viable option for application in a

peer-to-peer digitized voting system, beyond the traditional blockchain application domain in currency and finance. This drive is due to blockchain's perceived security, transparency, verification and compliance attributes in a distributed environment, that could address shortcomings inherent in e-voting systems.

Blockchain is a peer-to-peer (P2P) distributed ledge technology (DLT) for transparent transaction devoid of a trusted middleman that leverages on the internet, originally developed for crypto-currency virtual currency transactions. The initial focus of blockchain was in the financial sector, but it currently has applications in numerous areas majorly to enhance cybersecurity. Blockchain is defined as *an appendable immutable universally distributed open ledger* [12]. The key elements of this definition rests with the keywords: Here *apendable* means can add to the ledger, *immutable* means nothing can be deleted or altered from the ledger, *universally distributed* means equal accessibility of everyone to the same copy of the ledger each time information is updated to ensure validity of all transactions, which makes blockchain trustworthy and an open ledger database where all transactions are recorded in a clear, shared and transparent manner. The transformation blockchain is envisioned to bring to society will potentially be more than the internet. Whereas internet changed the way information is shared, blockchain will potentially transform the way transactions are done, with trust as a core ingredient.

Blockchain finds viable application potentials in many fields such as in education [13], healthcare system [14], smart cities [15], electricity industry [16-18], legal industry [19], Industry 4.0 [20-22], music industry [23], eGovernment to fight corruption and poverty [24], tax administration [25], in Agriculture through direct funding to farmers [26], charity and NGO to establish direct link between the donor and donee [27, 28] and electronic voting [1, 9, 29, 30], and so many other areas that rely on third party to establish trust. Blockchain is therefore, evolving beyond its initial application in currency and in the financial sector to other numerous domains collectively referred to as Blockchain version 3.0. The summary of these evolving blockchain application domains are outlined in Table 1.

TABLE I. EVOLVING BLOCKCHAIN APPLICATION DOMAINS [31]

Blockchain 1.0	Currency	Bitcoin, Litecoin, Ethereum, etc.
Blockchain 2.0	Banking & financial services, smart contracts, economics and financial market	Smart contracts, Smart property and asset
Blockchain 3.0	Beyond Blockchain 1.0 and Blockchain 2.0	Domain name, digital identity, eGovernment, IoT, smart cities, Industry 4.0, online electronic voting, among others.

As reported in [32], Sierra Leone took a bold but cautious step towards utilizing blockchain-based distributed ledger technology, by leveraging on blockchain-based digital voting platform owned by a Swedish start-up company called Agora, to store and verify the votes cast during the country's presidential elections. The country however still maintained the same paper-based ballot casting process it has employed in past elections. The process includes manual verification of voters' relevant identification documents and casting of their ballots. Subsequently, the voting results were then manually recorded into Agora permissioned blockchain platform, with Agora appointed by relevant stakeholders to act as the party to validate the data contained inside the network. Two main positives came out of this process, timely delivery of results and avoidance of fallouts or violence associated with electioneering processes in the country. Even though Sierra Leone did not use the Agora blockchain platform for the entire voting process, it clearly epitomises that democratic advancement through fair and transparent elections could be achieved using blockchain technology in Africa.

According to Bitcoin Africa [33] and [34], a growing number of blockchain Financial Technology (FinTech) start-ups are springing up in Africa, mostly in the financial and non-cash remittance ecosystem. Some of these start-ups and their application domains are enumerated in Table 2. In the long run, a number of these start-ups will eventually venture into other application domains driven by opportunities to solve numerous problems in the region. Including BEEV because of high stakes associated with elections thereby improving trust and transparency.

The rest of this paper is organized as follows: section II overviews blockchain concepts and DLT consensus approaches. Section III reviews the literature on electronic voting and its peculiarity in a developing country like Nigeria. Section IV reviews literature in blockchain voting systems. Section V discusses and highlight's Artificial Intelligence as an enhancer of blockchain technology. Section VI examines blockchain e-voting adoption in Nigeria using a qualitative SWOT and PEST analyses. Section VII concludes the paper.

II. OVERVIEW OF BLOCKCHAIN CONCEPTS

Blockchain is an integrated technology made up of several concepts and techniques such as cryptography, mathematics, economic model, and P2P networks based on distributed consensus algorithm [35]. Generally, there are three types of blockchain technology namely, 1) Public blockchain – everyone got assess to transactions and are stakeholders in attaining consensus, as a *permmissionless* blockchain with no centralized authority required for the verification process. Bitcoin and Ethereum are examples of public blockchain; 2) Private blockchain – There are restrictions on the distributed ledger data access, which is controlled by a few designated authorities, usually owned by an individual, government or private business. It operates as a permissioned blockchain with a central authority for process verification; 3) Consortium blockchain – This is a hybrid blockchain implementation which can be private or public. But assess to distributed ledger data is *permissioned*. Examples are Eris and Hyperledger.

Secure Hash Algorithm (SHA-256) encryption is the most used encryption and mostly associated with Blockchain, due to the unique attribute of its Hash function which produces unique outputs when specified by different

inputs. A Hash function is the private and public key uniquely created to identify an individual at the same time preserving privacy. It was originally developed by United States National Security Agency (NSA) to ensure uniqueness of codes [9]. Fig. 1 depicts the logic flow of SHA-256 encryption representation. A SHA-256 is made up of 256-bit encryption, 32 bytes, and 64 alphanumeric characters long every time. For example, an input plaintext of *Blockchain* and *blockchain* yields uniquely different hash keys, even with just difference of the first letter capitalised:

Blockchain:
625DA44E4EAF58D61CF048D168AA6F5E492DEA166D8BB54EC06C30DE07DB57E1

blockchain:
EF7797E13D3A75526946A3BCF00DAEC9FC9C9C4D51DDC7CC5DF888F74DD434D1

TABLE II. BLOCKCHAIN TECHNOLOGY START-UPS IN AFRICA

Start-ups	Network Consensus Platforms	Country	Application Domain
Blockchain Academy	Bitcoin/Stellar/Ethereum/IPFS/Hybrid systems	South Africa	Education/Social Engagement
Satoshicentre		Botswana	Education/Training/Social Projects
Wala		Uganda	Finance
BitPesa		Kenya	Finance/Forex Transactions
BitGive		US based (But with partnership operations in Africa)	NGO/Charitable Organization/Philanthropy
SureRemit		Nigeria	Finance/non-cash Remittance
Custos Media Technologies		South Africa	Media & Music Industry piracy
Kobocoin		Nigeria	Finance/payment system
Cryptogene		Nigeria	Education/Training
BitMari		Zimbabwe	Finance/Forex Transactions
ChamaPesa		Kenya	Library/Bookkeeping system
NairaEx		Nigeria	Finance/Exchange & remittance
Bankymoon		South Africa	Energy & Utilities payments/Smart grid/consultancy
BitFinance		Zimbabwe	Finance/ non-cash Remittance
The Sun Exchange		South Africa	Solar energy marketplace connect platform
Bitland		Ghana	Land & properties registry
GeoPay		South Africa	Finance/Forex remittance
OTLW		Kenya	Online Educational system

However, there are other cryptographic algorithms that are in use in electronic voting systems. Like RSA public key cryptography, Zero-knowledge-proof, Homomorphic encryption, Mix-nets scheme, Secret sharing and Threshold encryption, Everlasting privacy, and Blind signatures. For details, readers are referred to [1].

The structure of blockchain is basically made up of the block header and block body. The block header is made up encrypted unique hashes, while the block body is made of transaction counters and transactions saved in a block [9]. A summarised structure of the blockchain block structure is highlighted in Table 3 [9].

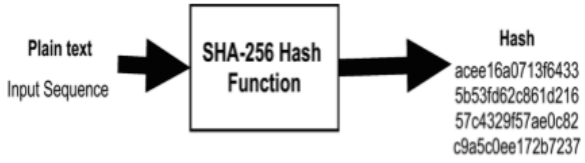

Figure 1. SHA-256 Hash Function Logic Representation

TABLE III. BLOCKCHAIN SINGLE BLOCK STRUCTURE

Field	Description
Block Header (size=80 bytes)	
Block version	Shows the block validation rules
Parent Block Hash	A 256-bit hash value that references the preceding block
Merkle Tree Root Hash	A Hash value of all transactions in the bock
Timestamp	Up-to-date transaction time stamp in seconds
nBits	Up-to-date hashing target in a compact format
Nonce	4-byte field, starting from 0 and grows for each hash calculation
Block Body	
Transaction counter	Number of transactions that follow as T_{X1}, T_{X2} …. T_{Xn} (size = 1-9 bytes)
Transactions	Number of transactions a block can contain depends on block and transaction size

A. Distributed Ledger Consensus Approaches

The key technical challenge in Distributed Ledger Technology (DLT) is the process of reaching consensus. When a community of computers or nodes on the network need to reach an agreement on how transactions happen, and the information updated in the distributed ledger without trusting any one single computer or node. In order words, it is a way of deciding who in the community of computers has a right to add the next block onto the blockchain through arriving at a mathematical solution on supercomputers, to avoid chaos on the chain. The whole idea is to have a ledger forming a fine single-chain as blocks are added to the blockchain, rather than a chaotic tree-like blockchain, which results to a massive amount of wasted energy on computation and no consensus attained. This chaotic tree-like occurrence is technically referred to as forks. The specific technical challenges include high computational cost, massive energy consumption, scalability, transaction throughput and speed, security and fairness in reaching a consensus. In the following subsections, we shall discuss the major distributed ledger consensus protocols and approaches.

1) Proof-of-work (PoW)

PoW was started and popularised by Bitcoin [36], it is based on the mechanism, where the longest block full of

transactions is added to the next block. The drawbacks of this approach are the high computational cost associated with reaching a consensus and the massive amount of electrical energy needed by the supercomputers in the processes. There is also the issue of scalability and transaction throughput per second. With this bitcoin-based protocol, only seven transactions per second are feasible. On the order hand, some experts are of the opinion that the slowness is for security reasons, to allow all nodes verify all transactions and allow time to agree on a consensus, in the process ensuring fairness and averting a fork. But with transactions such as in financial markets or stock exchanges where thousands of transactions occur per second, there is the need to scale up the transaction throughput from what is obtainable with this bitcoin protocol. Even though security experts believe that a combination of PoW with nonce value and SHA-256 hashes translate to high security, there remain other problems associated with PoW systems, such as improving scalability and better consensus reaching mechanisms. These challenges inherent with PoW motivates researchers to find new consensus approaches [37].

2) Leader-based system (LBS)

In LBS, all nodes in the network inform a designated leader of their transactions, the leader then decides on the order of transaction and notifies the entire network. However, there are security challenges with this approach. Scenarios could be a deliberate distributed denial of service (DDoS) virus attack on the designated leader, which will lead to total system collapse. Examples of Leader-based systems are PBFT, Raft and Paxos.

3) Proof-of-stake (PoS)

PoS is usually referred to as economy-based systems. It is an approach where the community of nodes vote based on what they think the consensus would be, by voting with the majority. The idea here is to observe carefully voting patterns of other nodes on the network and vote with the majority to reach consensus. It is called economy-cased system because it is likened to Adams Smiths theory of moral sentiments in economics, as voting judgement is inspired by sentiments merely observing how the majority are voting. It is more like sympathy voting. PoS consumes less energy compared to PoW and assumption that trustworthy nodes control at least 51% of network mining power to ensure a secure system. However, there are the possibilities of collusion by bad stakeholders to gather the required 51% mining power. This raises the question of how secured the system is. Its main drawback is nothing at stake problem. Owing to these challenges new PoS protocols have been designed and proposed such as delegated proof of stake (DPoS) and other hybrid systems of PoW, LBS and PoS, by combining the advantages of these protocols.

4) Voting-based system

This is a consensus reaching protocol where an individual node sends a vote over the internet, which make it a theoretical extremely slow approach. Hence, it has found very little real-world application.

At this junction, based on the consensus protocols described above. It is pertinent to briefly introduce the concept of Byzantine Fault Tolerant (BFT) [38]. BFT means the moment in time during transactions when it is clear that consensus is approaching and when consensus is attained and the mathematical surety that all nodes will reach exact consensus. BFT can either be asynchronous Byzantine (aBFT) or partly asynchronous Byzantine (paBFT), depending on the prior assumptions about existence and non-existence of trustworthy stakeholders in the network environment. With aBFT assuming that there exist untrustworthy nodes in the network environment and paBFT assuming otherwise.

5) Hashgraph

Hashgraph is a fully aBFT, based on the mathematical assumptions that consensus will be attained if less than one-third of the nodes are untrustworthy. Hashgraph leverages on a gossip protocol to send messages to all computer nodes on every transaction sent and received on the network to facilitate a quicker time of reaching a consensus agreement. It is essentially sending two compressed hash messages by a node to the next node, eventually forming a complete history of all communication in the entire network, referred to as *hashgraph in memory*. With aBFT based consensus protocols, like the hashgraph, there is higher surety that consensus is going to be reached as opposed to non-byzantine based protocols like PoW or PoS, which merely based on confidence level over time. Hashgraph addresses the concerns associated with PoW, these are increased scalability and transactions throughput, significantly lower computational overhead and power consumption and security. Readers are referred to [39, 40] for details on blockchain consensus models.

III. ELECTRONIC VOTING SYSTEM

A. Global View of Electronic Voting Systems

Estonia, Norway, New South Wales, and Washington D.C. in the US are a few countries around the world utilizing internet electronic voting systems. However, despite the advantages with e-voting systems, there are still security concerns bordering on transparency and centralization of the systems [1, 9]. Such security issues are still the only major factors slowing down its adoption in other developed democracies such as France and UK.

B. Existing Voting System in Nigeria

The conduct of the general election in Nigeria before 2015 election was manually driven with a high level of electoral fraud by electoral authorities, government authorities, political gladiators and erring voters [41]. However, the year 2015 witnessed the embrace of application of electronic voting technology to authenticate and validate voters. This application of Information and Communication Technology (ICT) brought partial sanity to democratic decision-making process but with salient socio-technical issues such as failed Smart Card Readers (SCRs) [42]; Subscriber Identification Module (SIM) issues [43]; Voter's biometrics fingerprint verification issues [14]. While the proposal for the automation of the voter's identification and verification could not be approved by the parliamentary screening for 2015 election, the aftermath of the application

continues to generate momentum and will eventually reverberate sooner or later if necessary examinations of previous and possible security threats are not anticipated and solved before future elections [3, 41, 44].

The recent legislative amendment of the Electoral Act by the Nigerian Senate empowering the country's Independent National Electoral Commission (INEC) to introduce and implement any e-voting technology it deems suitable [45, 46], is a good development towards the conduct of future elections and the possible adoption of BEEV in Nigeria.

IV. BLOCKCHAIN BASED VOTING SYSTEM

There are a few organization currently attempting to build BEEV solutions such as Civitas, Helios, TIVI, FollowMyVote, Bitcongress, Votecoin and Kaspersky Lab Business Incubator's secure online voting based on blockchain called Polys [47]. Most of these solutions are still in the developmental stages. Some works on BEEV in literature are briefly described as follows and summarized in Table 4:

In [9], the authors conceptualize a BEEV system to meet the requirements of authentication, anonymity, accuracy and verifiability. With the first vote cast, the first transaction added to the block and referred to as the foundation block, which contains the elected candidate's name, on which other votes for that candidate are built on and voting transactions update for every casted vote. The system also made provision for blank or protest vote, however, the system allows voting only once, which makes it impossible to change vote in case of a mistake. A general representation of the system from requesting to vote, authentication and vote casting, encryption and adding a vote to blockchain is depicted in Fig. 2.

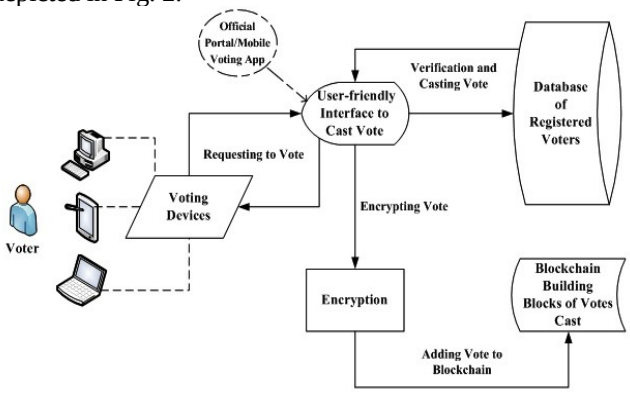

Figure 2. Conceptual BEEV Framework [9]

In [1] a modified PoS consensus protocol with less computational overhead compared to PoW for a web-based BEEV system using Homomorphic with a threshold-encryption scheme is proposed. The author utilises a proprietary defined blockchain protocol named a *Ballotcoin*, as against using Bitcoin protocol since a different consensus method is proposed and implemented.

The researchers in [48] proposed a BEEV system using blind signature encryption method for protecting voters' choices during elections. The authors claim that the solution satisfies all e-voting requirements, except the coercion-resistance attribute, which was challenging to implement due to the desirable transparency property of blockchain.

V. ARTIFICIAL INTELLIGENCE AS AN ENHANCER OF BLOCKCHAIN TECHNOLOGY

Artificial intelligence (AI) and blockchain are two technologies that are potentially going to revolutionize society. As they have found global acceptance across all industries. From data analytics on Google or Microsoft platforms to the banking and financial sectors, as well as in smart cities, were they are being increasingly utilized. In blockchain, data is stored in an encrypted distributed ledger format across numerous computers, hence the need for new AI techniques that will be able to analyze and make sense of data stored in this format. Blockchain technology is not entirely immune to cybersecurity and software bugs, because human programmers are central in the development and deployment of blockchain systems [49], in addition to known flaws associated with encryption algorithms [1] and the frequent cyber-attack on bitcoin blockchain systems. An example will be a situation where the shortest chains are deliberately extended as oppose to longest block full of transactions to be added to the next block, leading to system collapse. Owing to these arguments the decentralized attributes of blockchain does not entirely hold. Going forward, numerous researchers are of the consensus that the security and other attributes of blockchain technology can be greatly enhanced by leveraging on AI techniques.

VI. BLOCKCHAIN E-VOTING ADOPTION ANALYSIS IN NIGERIA USING SWOT AND PEST FRAMEWORKS

In this section, we employ a combination of SWOT and PEST analytical approaches based on a similar work by [50], to assess the current state and prospects of BEEV system in Nigeria. We assess internal and external factors in ***Strengths***, ***Weaknesses***, ***Opportunities***, and ***Threats*** in relation to ***Political, Economic, Social*** **and** ***Technological*** influencing factors. It is outlined and summarized in Table 5.

TABLE IV. SUMMARY OF SOME SURVEYS OF BLOCKCHAIN IN ELECTRONIC VOTING

Study	Blockchain Architecture	Type of Blockchain	Platform Network	Encryption Hash Function	Consensus Method
[9]	Permissionless	Public	Bitcoin	SHA-256	PoW (longest chain rule)
[1]	Permissionless	Public	Ballotcoin	Homomorphic with threshold-encryption	Modified PoS
[48]	Permissioned	Public	Bitcoin	Blind signature	Not specified

TABLE V. A SUMMARY OF SWOT AND PEST ANALYSIS OF BEEV IN NIGERIA

SWOT/PEST	Strength	Weaknesses	Opportunities	Threats
Political	○ Relatively stable and maturing democracy since 1999 ○ Vibrant legal and democratic experts to leverage on in driving the democratic process ○ Cooperation between public and the private sector in issues such a public education mobilization, blockchain providers and government institutions	○ Lack of political will to adopt new technology and reluctance to invest in blockchain technology ○ Suspicious public on Government policies and distrust in elections ○ Weak legal regulatory frameworks and weak political will to enact cybersecurity laws ○ Lack of favorable government policies on blockchain technology and start-ups ○ Poor policy implementation ○ Weak political structures and incumbency power	○ Economic inclusiveness & globalization and pressure for diaspora voting ○ Tested scenarios such as Estonia & Sierra Leone to motivate Nigeria government ○ Greater interest by the regional and global organization for a better democratic system in developing democracies	○ Insecurity, such as Boko Haram terrorism, kidnapping etc. ○ Foreign political interference ○ Cyber-terrorism and hacking
Economic	○ Already huge existing investments in infrastructures ○ A large pool of IT-savvy population to drive the process, such as young NYSC graduates ○ Government huge budget allocation to INEC ○ Competition among internet service providers (ISP) has driven the cost of internet subscription low	○ Insecurity taking a substantial amount of resource ○ Over-dependence on oil revenue (monolithic economy)	○ Cost reduction by the government on elections due to dwindling oil income ○ Foreign institutions' /Governments interest and funding of democratic processes	○ The high cost of internet subscription due to infrastructural challenges as power supply and rising fuel prices burden of ISP ○ Fluctuating international oil price
Social	○ Improved IT literacy ○ Urbanization ○ Growing middle-class population ○ The booming mobile phone market ○ Leveraging on the diaspora and foreign experts	○ Fragile political system prone to violence and intimidation and general insecurity ○ Low IT literacy level of especially older generation, that may be discouraged and thereby disenfranchised ○ Public education and winning trust/buy in	○ Insecurity situation usually during an election period, will encourage online voting system. ○ High Smartphone adoption and usage ○ Difficult topographical terrain could motivate blockchain-enabled e-voting ○ Increasing clamor and agitation for credible elections by citizens	○ Possible disenfranchisement of the non-literate voting population by using blockchain technology ○ Social Engineering to compromise voters' devices ○ Traditional, cultural and religious beliefs
Technology	○ Improved telecommunication services ○ Innovation through blockchain start-ups for a tailored technology to suit peculiarities ○ Foreign-based IT experts ○ Vibrant high-tech based youth population	○ Low internet penetration level ○ Poor voters' database ○ Overcapacity of the internet during elections due to heavy traffic ○ Preparedness of electoral body's IT infrastructure to handle elections ○ Power supply challenges ○ Less IT-savvy population	○ Improved broadband connectivity ○ Growing number of ISP players to provide competition and redundancy ○ Improved cloud services	○ Programmers coding that builds blockchain prone systems to bugs and possibilities of hacking ○ Due to dependency on IT, any little technical problem could affect the entire network & disrupt the process ○ Meddling into the election by foreign powers via cyber means ○ Standardization to enable interoperability between blockchain ledgers & existing legacy systems ○ No known fully large-scaled BEEV to leverage on is in place. ○ Malware attack or lost of voter's device.

A. *Summary Remarks of SWOT and PEST Analysis*

Blockchain is still at the developmental stage in Nigeria, with early application entry mainly in the banking and financial sectors driven by fintech innovators. This is an early good sign for blockchain future development in other application domains for Nigeria including in BEEV. However, the overall future of BEEV system is still in its incubation phase. But, if governments wish to adopt blockchain based voting, they would need to invest resources and most likely partner with the private fintech companies for a tailored BEEV system for the region. Adoption will depend on a favourable political, economic and technological environment in Nigeria and the entire African region, as clearly shown in Table 5. Internet voting will inevitably be an option in the near future using smartphone devices or other electronic machines, and blockchain technology can be of great assistance for voting to become secure.

VII. CONCLUSION AND FUTURE WORK

The internet pioneers initial vision was an independent and decentralised platform for information sharing, but over the years the internet has become too centralised and managed by a few tech giants such as Google. Will blockchain suffer the same fate? Only time will tell. Even though blockchain faces several challenges such as security concerns, software bugs, inadequate legal and regulatory frameworks etc. It is the authors' opinion that careful implementation of blockchain technology in the democracy of developing countries adhering to the troika pillars of people, processes and technology, could usher in peace, stability and sustainable development. However, adoption must be done gradually. We observe that most BEEV works in literature are mostly theoretical and remains to be tried and evaluated in a large-scale real-world scenario. A mixed approach of existing voting systems and blockchain is proposed in the context of Nigeria for the short and medium term. We also emphasise a tailored BEEV for developing democracies taking into consideration, security and data integrity in fairness to scalability, flexibility and complexity of blockchain architectural design choices that will be user-friendly. Finally, it will be interesting to apply a quantitative SWOT and PEST analysis in addition to incorporating stakeholders' support and expectations to evaluate BEEV in Nigeria. This is an open issue for future research endeavours.

ACKNOWLEDGMENT

This work was supported by the Department of Electrical and Electronic Engineering Science at the University of Johannesburg, South Africa.

REFERENCES

[1] C. Meter, *"Design of Distributed Voting Systems"*, MSc Thesis, Department of Computer Science, Heinrich-Heine-Universität Düsseldorf, September 2015, Retrieved from https://arxiv.org/pdf/1702.02566.pdf, on 20 March 2018.

[2] O.M. Olaniyi, O.T. Arulogun and E.O. Omidiora, "Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting", *African Journal of Computing and ICT*, vol. 5, no. 6, pp. 10-16, Dec. 2012.

[3] B.A. Oke, O.M. Olaniyi, A.A. Aboaba and O.T. Arulogun, "Developing Multifactor Authentication Technique for Secure Electronic Voting System", *Proceedings of IEEE International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1-6, Covenant University, Otta, Nigeria, 2017. doi: 10.1109/ICCNI.2017.8123773.

[4] S. Ibrahim, M. Kamat, M. Salleh and S.R.A. Aziz, "Secure E-voting with Blind Signature", *Proceedings of the 2003 4th National Conference of Telecommunication Technology, (NCTT2003)*, pp. 193-197, 2003. doi: 10.1109/NCTT.2003.1188334

[5] Jinn-Ke Jan, Yu-Yi Chen and Yi Lin, "The Design of Protocol for e-voting on the Internet," *Proceedings of the 2001 IEEE 35th Annual International Carnahan Conference on Security Technology (Cat. No.01CH37186)*, pp. 180-189, London, 2001.

[6] L. Chiang, "Trust and security in the e-voting system", *Electronic Government, an International Journal (EG)*, vol. 6, no. 4, pp. 343-360, Aug 11, 2009.

[7] D.L. Dill and A.D. Rubin, "E-voting Security", *in IEEE Security & Privacy*, vol. 2, no. 1, pp. 22-23, Jan.-Feb. 2004. doi: 10.1109/MSECP.2004.1264849

[8] M. Shamos and A. Yasinsac, "Realities of E-voting Security*", in IEEE Security & Privacy*, vol. 10, no. 5, pp. 16-17, Sept.-Oct. 2012. doi: 10.1109/MSP.2012.124

[9] Ahmed Ben Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System", *International Journal of Network Security & its Applications (IJNSA)*, vol. 9, no. 3, May 2017.

[10] Y. Wu, *"An E-voting System Based on Blockchain and Ring Signature"*, MSc Thesis, Department of Computer Science, University of Birmingham, 2017, Retrieved from https://www.dgalindo.es/mscprojects/yifan.pdf, on 14 July 2018

[11] W. Al-Saqaf and N. Seidler, "Blockchain Technology for Social Impact: Opportunities and Challenges Ahead", *Journal of Cyber Policy*, vol. 2, issue 3, pp. 338-354, 2017.

[12] K. Kimbel, "The Secret Behind the Blockchain Technology", in March 21st, 2018 PECB Webinar presentation. Available online at, https://pecb.com/past-webinars/the-secret-behind-the-blockchain-technology

[13] J. Rooksby and K. Dimitrov, "Trustless Education? A Blockchain System for University Grades", *Paper presented at New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS2017*, 10th June 2017, Edinburgh. Retrieved from http://johnrooksby.org/papers/DAOworkshop_rooksby.pdf, on 20 May 2017

[14] T. Kuo, H. Kim and L. Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Healthcare Applications", *Journal of the American Medical Informatics Association*, vol. 24, issues 6, 2017, pp. 1211-1220. https://doi.org/10.1093/jamia/ocx068

[15] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology", *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 1392-1393, Sydney, NSW, 2016. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198

[16] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie and M. Bertoncini, "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids", *Sensors*, vol. 18, no. 1, Article no. 162, 2018. doi:10.3390/s18010162

[17] L.W. Park, S. Lee and H. Chang, "A Sustainable Home Energy Prosumer-Chain Methodology with Energy Tags over the Blockchain", *Sustainability, MDPI, Open Access Journal*, vol. 10, no. 3, pp. 1-18, Mar 1, 2018. doi:10.3390/su10030658

[18] J.J. Sikorski, J. Haughton and M. Kraft, "Blockchain Technology in the Chemical Industry: Machine-to-Machine Electricity Market," *Applied Energy, Elsevier*, vol. 195(C), pp. 234-246, 2017. doi: 10.1016/j.apenergy.2017.03.039

[19] D. Dontsov, "How Blockchain Technology Can Drive the Legal Industry Forward", *Law Journal Newsletters*, Jan. 2018, Retrieved at http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2018/01/01/how-blockchain-technology-can-drive-the-legal-industry-forward/?slreturn=20180614094636, on 20 April2018.

[20] A. Bahga and V.K. Madisetti, "Blockchain Platform for Industrial Internet of Things", *Journal of Software Engineering & Applications*, vol. 9, no. 10, pp. 533-546, 2016. doi: 10.4236/jsea.2016.910036

[21] E. Hofmann and M. Rusch, "Industry 4.0 and the Current Status as Well as Future Prospects on Logistics," *Computers in Industry: An International Journal*, vol. 89, pp. 23-24, August 1, 2017. doi:10.1016/j.compind.2017.04.002

[22] K. Rabah, "Overview of Blockchain as the Engine of the 4th Industrial Revolution", *Mara Research Journal of Business and Management*, vol. 1, no. 1, pp. 125-135, Sept. 2016. ISSN 2519-1381

[23] M. O'Dair, Z. Beaven, D. Neilson, R. Osborne and P. Pacifico, "Music on the Blockchain", Report no. 1, Middlesex University, 2016, Retrieved from https://www.mdx.ac.uk/data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf, on 14 April 2018

[24] S. Ølnes, J. Ubacht and M. Janssen, "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing," *Government Information Quarterly*, vol. 34, pp. 355-364, Sept. 2017.

[25] Deloitte, "Blockchain Technology and its Potential in Taxes", December 2017. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF, on 14 April 2018

[26] L. Ge, C. Brewster, J. Spek, A. Smeenk, J. Top, V. Diepen Frans, B. Klaase, C. Graumans and Ruyter de Wildt, de, Marieke, "Blockchain for Agriculture and Food; Findings from Pilot Study", *Wageningen, Wageningen Economic Research*., Report 2017-112, 2017. doi.org/10.18174/426747

[27] Charities Aid Foundation, "Giving Unchained: Philanthropy and the Blockchain", Giving Thought Discussion paper no.4, December 2015. Retrieved from https://www.cafonline.org/docs/default-source/about-us-publications/givingunchained-philanthropy-and-the-blockchain.pdf?sfvrsn=4, on 10 April 2018

[28] Charities Aid Foundation, "Blockchain Technology Could Revolutionise Charitable Giving - Report", December 2015. Retrieved from https://www.cafonline.org/about-us/media-office/blockchain-technology-could-revolutionise-charitable-giving, on 10 April 2018

[29] S. Bistarelli, M. Mantilacci, P. Santancini and F. Santini, "An End-to-End Voting-System Based on Bitcoin," *In: Proceedings of the Symposium on Applied Computing, SAC '17*, Marrakech, Morocco, pp. 1836-1841, Apr 3-7, 2017.

[30] K. Hegadekatti, "Analysis of Present Day Election Processes vis-a-vis Elections Through Blockchain Technology", *Munich Personal RePEc Archive, MPRA*, Paper no. 82866, Nov. 2017.

[31] J. Lluis de la Rosa, V. Torres-Padrosa, A. el-Fakdi, D. Gibovic, O. Hornyák, L. Maicher and F. Miralles, "A Survey of Blockchain Technologies For Open Innovation", *4th Annual World Open Innovation Conference*, San Francisco, CA, Dec. 14-15, 2017.

[32] A. Lielacher, "Sierra Leone Successfully Holds World's First Blockchain-Enabled Election," Bitcoin Africa, March 9, 2018, Retrieved from https://bitcoinafrica.io/2018/03/09/sierra-leone-blockchain-election/, on 10 April 2018

[33] Bitcoin Africa, "African's Blockchain Startups", 2017, Retrieved from https://bitcoinafrica.io/category/meet-africas-blockchain-startups/, on 10 April 2018

[34] UN Economic Commission for Africa, "Blockchain Technology in Africa", United Nations Expert Group Meeting in Addis Ababa, Ethiopia, Nov. 21-22, 2017. Retrieved from https://www.uneca.org/sites/default/files/images/e1701284_concept_note_egm_22_november_2017.pdf, on 10 April 2018

[35] I-C. Lin and T-C. Liao, "A Survey of Blockchain Security Issues and Challenges", *International Journal of Network Security*, vol. 19, no. 5, pp. 653-659, Sept. 2017. doi: 10.6633/IJNS.201709.19(5).01

[36] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Retrieved from http://bitcoin.org/bitcoin.pdf, on 20 March 2018

[37] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication", In: Camenisch J., Kesdoğan D. (eds) *Open Problems in Network Security, (iNetSec2015)*, Lecture Notes in Computer Science, vol. 9591, pp. 112-125, 2016. doi:10.1007/978-3-319-39028-4_9

[38] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance", *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, pp. 173-186, New Orleans, Louisiana, USA, Feb. 1999.

[39] A. Baliga, "Understanding Blockchain Consensus Models", Persistent Systems Ltd., White paper, 2017, Retrieved from https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf 2017, on 20 March 2018.

[40] N. Chalaemwongwan and W. Kurutach, "State of the Art and Challenges Facing Consensus Protocols on Blockchain", In: *2018 International Conference on Information Networking (ICOIN)*, pp. 957-962, Chiang Mai, Thailand, 2018. doi:10.1109/ICOIN.2018.8343266

[41] O.M. Olaniyi, O.T. Arulogun, E.O. Omidiora and O.O. Okediran, "Enhanced Stegano-Cryptographic Model for Secure Electronic Voting", *Journal of Information Engineering and Applications (JIEA)*, vol. 5, no.4, pp. 1-15, 2015.

[42] O. Osho, V.L. Yisa and O.J. Jebutu, "E-voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors*", In: 2015 International Conference on Cyberspace Governance (CYBER-Abuja)*, pp. 202–211, 2015.

[43] Vanguard Nigeria, "After Initial Card Reader Failure - Nigerians Persevere, Vote in Peaceful Elections", March 29, 2015, Retrieved from https://www.vanguardngr.com/2015/03/after-initial-card-reader-failure-nigerians-persevere-vote-in-peaceful-elections/, on Mar 30, 2019.

[44] S. Ahmad, S.A.J. Abdullah and R. Bt. Arshad, "Participation and Voting Policy Process in Nigeria: A Qualitative Study", *Mediterranean Journal of Social Sciences*, vol. 6, no. 4, pp. 362-374, 2015.

[45] Policy and Legal Advocacy Centre (PLAC), "Report of the Ad-hoc Committee on the Legislative Agenda", 2017, Retrieved from http://placng.org/wp/wp-content/uploads/2016/06/8TH-SENATE-DRAFT-LEGISLATIVE-AGENDA-2.7.15.pdf, on 15th April 2018.

[46] Verified Voting Foundation, "Senate Amends Electoral Act, Approves Electronic Voting," March 31 2017, Retrieved from https://thevotingnews.com/senate-amends-electoral-act-approves-electronic-voting-ynaija/, on 12th April 2018.

[47] I. Kubjas, "Using Blockchain for Enabling Internet Voting", 2017. Accessed online at https://pdfs.semanticscholar.org/8d92/1dbfe6bebefa2599ca6afc7eeae82210a71d.pdf, on April 10, 2018

[48] Y. Liu and Q. Wang, "An E-voting Protocol Based on Blockchain", *IACR Cryptology ePrint Archive*, vol. 2017, pp. 1043, 2017.

[49] T. Marwala and B. Xing, "Blockchain and Artificial Intelligence", *CoRR*, vol. abs/1802.04451, 2018, Retrieved from https://arxiv.org/ftp/arxiv/papers/1802/1802.04451.pdf, on 20 April 2018

[50] H. T. T. Ha and K. A. Coghill, "E-government in Singapore - A SWOT and PEST analysis," *Asia-Pacific Social Science Review*, vol. 6, no. 2, pp. 103-130, 2006.