Int. j. inf. tecnol.
https://doi.org/10.1007/s41870-020-00440-w

ORIGINAL RESEARCH

Blockchain technology for electoral process in Africa: a short review

Mahtab Alam[1] · **Mukhtar Opeyemi Yusuf**[1] · **Nazifi Alhassan Sani**[1]

Received: 21 May 2019 / Accepted: 29 January 2020

Abstract The electoral process has suffered from deep political instability following the post-colonial independence of most African nations. Moreover, the electoral process in many countries is characterized by massive rigging, high cost of electoral materials, and declaration of false results. In this paper, we will present a review of the blockchain Technology and some of the potential roles to play in conducting a transparent election. This paper opines that with the emergence of the blockchain technology, African Nations should tap from it and build a reliable, secure, and convenient electoral voting system. It further suggests that a blockchain electoral voting system will eliminate most of the challenges faced by African nations in conducting a free, fair and transparent election with low cost and total security. The issue of election rigging is almost completely eradicated with this technology (if properly installed). An attempt to alter/manipulate records (votes) in the system's database can be spotted easily, because of its rigorous consensus rules, such an attempt is considered void and denied permission to access, alter, or destroy any of the previously saved votes. However, the paper argues that there are institutional challenges to implementing this technology within the continent. Specifically, there is a need to educate the masses as well as create robust policies that can accommodate this technology within the continent. Failure to acknowledge these challenges may well prevent the application of blockchain technology in African electoral process in the foreseeable future.

Keywords Blockchain technology · Electoral process · Ballot-box · Voting system · Africa · Votes

1 Introduction

Africa indeed have suffered lots of backlashes in terms of political instabilities, and these backlashes have led to lots of epileptic development in all major sectors of governance. It became a space where most political aspirant make it a do-or-die affair to gain power and respect while these uncultured attitude towards democracy are vastly becoming a deep rot that spreads through various nations within it's bound, violence and coercion then become a traditional ingredient for acquiring power or changing power from major opposition parties, as such, the poor innocent unemployed youths are targeted and psychologically manipulated to become actors for most violent acts.

Many strategic attempts have been initiated by various nation's electoral commission to eliminate these set-backs and to carry out a free, fair and credible election. But over the years some of these attempts failed to completely solve some major problems like the vote rigging/result interference, which is still one of Africa's biggest electoral problem, where a party (especially the incumbent party) with all their enriched resources can consistently rig election votes to remain in power for a very long period of time especially where the constitution permits.

✉ Mahtab Alam
alam12mahtab@gmail.com

Mukhtar Opeyemi Yusuf
mukhtaropeyemi@gmail.com

Nazifi Alhassan Sani
nalhassansani@gmail.com

[1] Department of Computer Science, Noida International University, Plot 1, Yamuna Express Way, Sector 17A, Greater Noida, Uttar Pradesh 203201, India

Published online: 28 February 2020

Election rigging is not only an Africa-electoral problem, it's an undeniable problem in every part of the world where democracy is adopted. Some nations have carried this burden as their individual responsibility to see to a transparent, free, fair and credible election. In some nations, organizations collectively agree that if humans cannot be completely trusted, they could reduce the degree/level of human interference with the voting system by allowing machines and computers to take over most phases of verification/authentication, counting and public display of results for transparency. This practically did not give a complete secure electoral voting because they still at some level need human to carry out various processes, like data entry, system configuration and maintenance, and lots more. All these brings loophole for attackers to gain some level of access to the system and when this unauthorized person(s) gain access to a voter's verification detail they can pose as if they are the legitimate voter and disfranchise the real voter. But in their attempts they were able to solve the question of transparency to some certain level, unless the security system of the machine was breach they will be able to deliver a transparent electoral process. That uncertainty or possibility of security breach is too much of a risk for an opposition party to take, because this could mean party with the proper resource and expertise have the option of infiltrating the system. As a result, some nations were forced to reject this electronic-electoral system and return to their old traditional voting system while searching for a better solution to tackle their loose-ends.

Electronic voting machine have become a very large topic for debate over the last decade as most nations are pushing towards it but critics consistently argue about their concern in terms of the risk of implementing such powerful tool, most believed that if the *internet* is involved then it's not secure either from the client's end or server end.

How do we solve all this unending insecurities and yet make the voting system as public and transparent as possible? This have become the questions for all IT experts that engage in this topic. With the emerging blockchain technology, blockchain experts can agree with us that this technology is almost indestructible, provides high-end cryptography security, transparent and publicly verifiable. It is frequently utilized in numerous cash transactions such as, advanced resources, settlement, currency and direct peer-to-peer on-line payment [2, 3]. Moreover, it may be used into different areas as well as utilitarian agreements [4], public services [5], web of Things (IoT) [6], name systems [7] and security services [8]. This technology has shown its credibility over the last 8 years in cryptocurrency where it has grown to a multibillion-dollar market valued investment. Although some of this cryptocurrency platform like bitcoin have suffered some attacks resulting to some huge loss of money, this is because regardless of how flawless this technology may seem, if not properly implemented and maintained attackers are still viable to penetrate mostly from the client side (the user end). A few highlighted advantages of blockchain electoral voting system over the traditional voting system (ballot-box system), includes—It is safer and more convenient for both voters and electoral commission body to use and manage respectively. According to Madavi [9], he also stated that in a blockchain network "Once data is entered, cannot be changed or erased". Hence, Votes saved via the system are very well secured and almost impossible to alter. It is very transparent because the blockchain itself can be designed as a public immutable ledger. It is economically cheaper to run and maintain compared to the traditional ballot-box system.

With this technology properly integrated on the electoral processes in African nations, citizens can exercise their voting right with no fear of violence, interference or incredible results, complete anonymity of voters, all votes are public, amongst many more advantage some of which will be uncovered in the rest of the paper.

2 Proposed system requirement

To successfully implement a blockchain electoral voting system that efficiently serves the need of the people, the proposed system must meet up with some basic requirements. Few of these requirements are discussed below.

1 *Registration/authentication* nation's independent electoral commission should be able to gather voters' verified bio-data information before the electoral process. This may be in a form of using previously existing data pool of information like the citizen national identification card, or creating a permanent voter's card. Whichever choice of preference used, it must ensure that each voter's bio-data verification is accessible on its local network with high permission to only its verified ad-hoc staffs. Getting voter's information residing on a third-party network endangers the vulnerability of voter's information from been compromised.

2 *Voter's identity* According to Venkatapur et al. [10] they agreed that "Voter must always be anonymous in the voting process. The system must aim at achieving the political privacy". Therefore, high-end encryption techniques must be used to protect voter's identity. Voter and their respective votes must remain anonymous throughout and after the process of the election. Failure to provide this anonymity and confidence is an abuse to voter's right and in some cases endanger the voter's life.

3 *Transparency* the proposed system must be transparent enough to counter most problems faced by the existing system. In the proposed system, there exist a public ledger on every node across it's network that register all votes casted and providing necessary information to verify the authenticity of each vote but hiding the voter's personal information. Any changes or update to be made on the system must be agreeable and verifiable by all the node participant on the network.

4 *Security* comprehensive security guidelines defends organization from attacks as well as unintentional internal outflow of information, and data maladministration [11]. Strong security measures and techniques must be put in place to protect information shared across the network. Aside the high encryption technique that the blockchain provide, it also allows some security techniques like smart-contract, consensus, nonce, harsh of the previous block in every block, and many other techniques. Also the proposed system must be made all information stored in it indestructible and well protected.

3 Analysis of the existing system

Elections in Africa over many decades have been carried out using the ballot-box voting system, where voters are pre-registered prior to the election date, and on the day of election they arrive at the polling unit where they verify each voters by going through the records of registered voters and ticking out voter's name so he or she cannot vote more than once. After verification of voter, he/she is giving a ballot paper to cast their vote where they select their preferred candidate of choice and put the ballot paper in an enclosed/sealed ballot box. When the time giving to carry out the electoral process elapses, every ballot boxes are opened by the verified electoral commission staffs, and each ballot papers are counted according to respective candidate and in the end the candidate with the highest vote according to the ballot paper is considered the winner of the election.

This voting system is still in used in most part of African nations today, even though over the years its vulnerability has been exploited. Also due to the cost of development and implementations some nations find it difficult to adopt any new system of voting and rather continue to improve on tackling the issues vulnerable to the ballot-box system.

Some African nations have taken the challenge to tap into the electronic voting system, to enhance security and provide them with a clean fair election, some political analyst have considered this as a good step up in such nations but unfortunately this system does not answer all the questions especially regarding transparency and security. For example, in 2014 Namibia became the first African nation to adopt the electronic voting system, they introduced an electronic voting machine (EVM) that was developed and still in use by the Indians. According to the electoral commission of Namibia (ECN) there are some various challenges faced during the electoral process, but the major concerning issues to most analyst was the slow response of the VVDs (Voters verification device) which causes delay in queue for voters, while some analyst argue that this alone might have disfranchised some voters who are unable to withstand the stress of queuing up for too long [1]. Also in 2015, the Federal Republic of Nigeria introduced the electronic voting system by adding the biometric card reader to the registration and verification/authentication layer of its voting system, this makes it impossible for individual to cast a vote more than once, this step claim the victory of the country's first clean and fair election. But this system also like the EVMs used in Namibia's 2014 election had the technological failure of some voter card reader devices not responding, which also had the same effect as it did in Namibia. Another issues this two voting system have in common is that voters must commute back to their registration centers to be able to cast their votes, and citizens in diaspora or citizens that were not in the country for some reason don't have the avenue to cast their votes.

4 Design of the proposed system

Blockchain is a decentralized public ledger with strict-encrypted mechanism on its member interoperability. In a much simpler form, blockchain is simply a data structure of singly linked-list of nodes within a network, each nodes contains several blocks, each block holds cryptographic information of the previous block. Below is a simple overview representation of a blockchain network (Fig. 1).

Blockchain is a very complex technology even for some experts, for that only the important details that would be of interest to this paper will be discussed.

4.1 Consensus

Each node in a blockchain are also permissible to create a new block to the network, but there must be a well-defined consensus that guide them to perform such task. If all the requirements in the consensus are met by the new block, a copy of it is sent across the network to all participating blocks, if all blocks ones again accept this request then only a new block can be added to the network.

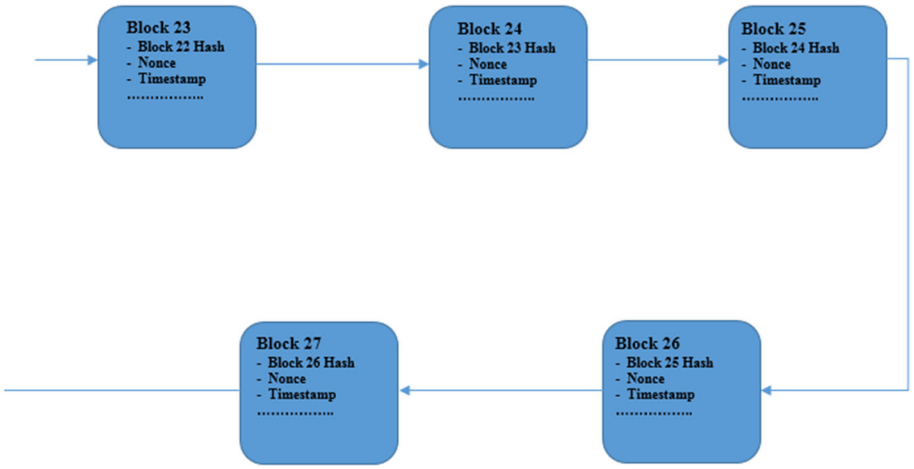

Fig. 1 Blockchain network structural representation

4.2 Smart contract

Every task carried out by different blocks in a network is supervised by a prebuilt well-defined document, this is referred to as smart contract, all blocks must contain a smart contract that define their role and how to carry out their process. Smart contracts are like encoded business contracts, and according to Blockchain Hub [12] "A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced."

4.3 Nonce

After all requirements are met with the consensus and the smart contract terms are agreed upon, a transaction is created and ready to be added to a block on the network. The transaction when ready would be encrypted with a harsh encryption. Nonce is a random 32-bit number that allows to generate (at the time of encryption) a specific number of leading zero's in the harsh of a particular transaction, this number of leading zero's in the harsh is known as the difficulty of the network and it is synonymous across all blocks in the network.

For example, below is a generated harsh from the string "My first block".

Your Hash: **b89a1b498c22d6464ddcfcf60bc96bb9**
Your String: My first block

The harsh of the string above is **b89a1b498c22d6464ddcfcf60bc96bb9** but if the blockchain network difficult level requires 4 leading zeros' then we need to find a random number that when added to the string will generate a harsh like this **0000b89a1b498c22d6464ddcfcf60bc96bb9**. This number is regarded as the nonce, and it only affect only that particular transaction, so if an attacker was able to guess a particular transaction's nonce, the attacker has to know every other nonce for the rest of the transaction. This is the simple concept of nonce.

In practical, every polling station represents a node in the network, every node carries out transactions which are publicly integrated to other blocks on the network for verification and public access.

Each polling unit will represent each node on the network, in case we have to trace any error we know where it's coming from. While each vote represents a block. This gives every voter the flexibility to vote from any polling unit within the nation, instead of having to travel back to their local polling unit to vote.

When the voter arrives at the polling unit, they undergo the verification process, where they have to successfully pass the biometric verification. On successful biometric clearance, the voter will proceed to the voting booth where he/she will have to vote their candidate of choice, once the vote is successfully acknowledged, a transaction is created and stored in a block on the blockchain ledger which will be distributed across all nodes for consensus check. This newly created block contains some important information, like the block number, harsh of the previous block (referencing immediate previous block), transactions (in this case votes and voter's credentials) and some other information that is not relevant to users. Information once stored on the blockchain ledger are permanent and cannot be altered, any attempt to alter an information on the ledger trigger all succeeding blocks as corrupt, because every block contains cryptographic information from its previous block. For example, the structure below shows what happens when a block information is tampered with.

Once an attempt is made to alter a particular block recording many votes in the ledger, the subsequent blocks

are affected, and this make it easier to trace where the problem is coming from as shown in Fig. 2. After some periodic fixed time, all nodes on the network are programmed to automatically exchange a copy of their current valid ledger with each other to keep them up-to-date. This exchange of ledger will then replace any damaged/faulty block and the whole network is backed up again. This technique makes the blockchain an exceptional in terms of security.

5 Workflow of the proposed system

In Fig. 3 we propose the basic workflow on working procedure for how the proposed system will work. The Actor signifies the voter, the voter arrives at the polling booth for verification and authentication. Electoral commission of each nation should be able to keep and update a comprehensive biometric record of its citizen, a dedicated biometric ID should be generated for each citizen, for example the biometric verification number (BVN) used in the financial system of Nigeria. This can partly be integrated into the proposed system, allowing voters that have been verified once for a particular vote session, unable to participate in another session elsewhere unless another voting category is selected. After verification of the biometric information of voter follows authentication during this phase voter's biometric ID is entered in the voting machine where voter will be allowed to vote for their candidate of choice. This biometric ID is again screened for the second time, if it exists in any node of the blockchain network, then voter will be restricted access to vote as it signifies voter's vote had already been counted somewhere. Successful authentication allows voter to continue with their voting process and vote casted are made public on the ledger across all nodes in network.

Figures 4 and 5 describes the first phase and second phase work of electoral commission respectively that how the proposed system will carry out their task phase wise.

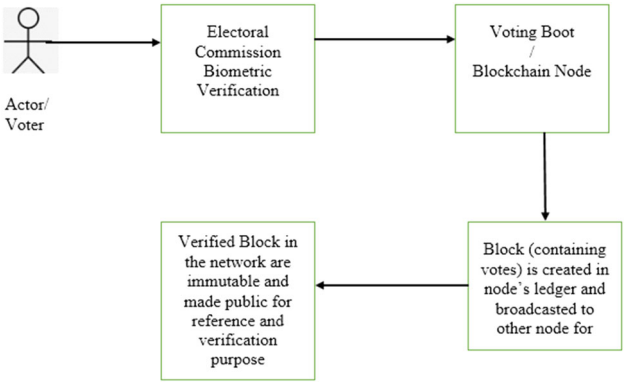

Fig. 3 Basic workflow idea

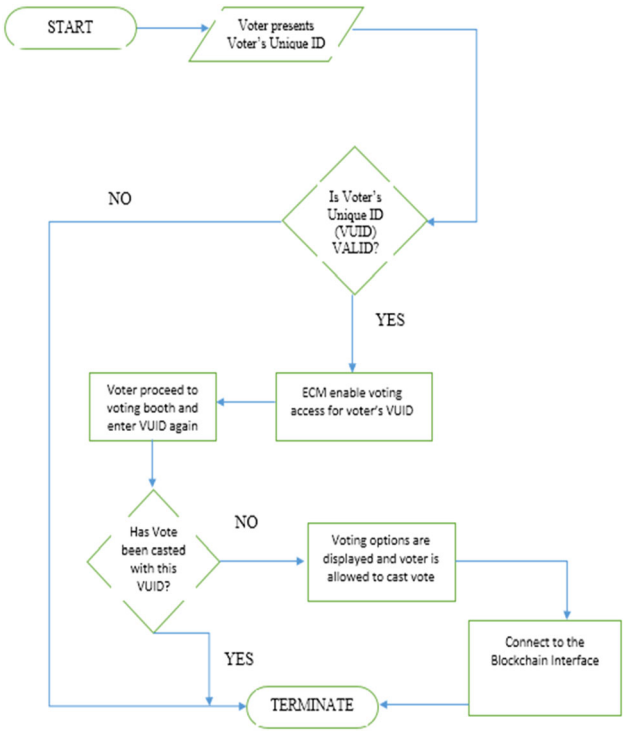

Fig. 4 Flowchart: first phase of electoral commission

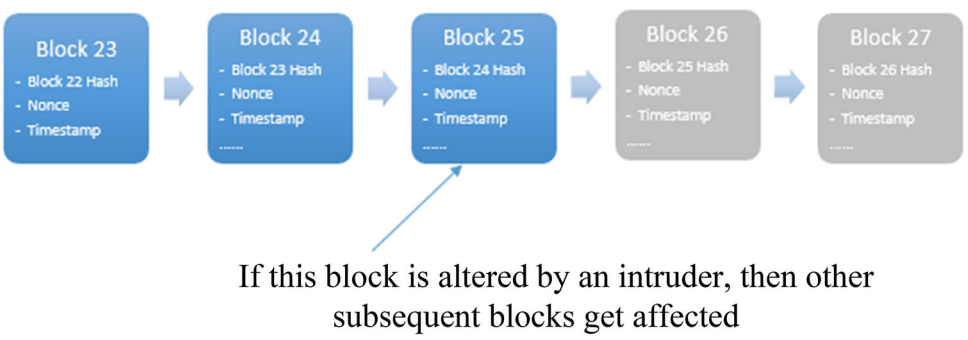

Fig. 2 Attackers disrupted chain of the blockchain

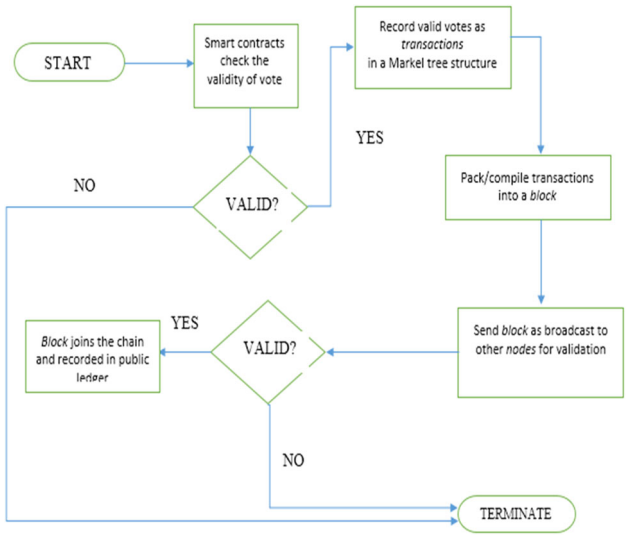

Fig. 5 Flowchart: second phase of electoral commission

6 Architecture of the proposed system

The Fig. 6 briefly explains the interaction within the blockchain network and some external actors. Permitted actors such as voters, external electoral observers, etc. can participate in the network from desired node and will have full participating feature according to their permissioned role in the network.

Ledger as we know stores chunks of verified blocks, each blocks holds certain amount of transactions (votes). Every node in the network have an exact copy of the ledger, and each ledger can be accessed by any permissioned actor in that node. Consensus mechanism ensures that communication and exchange of data within nodes are valid as it should be or discard otherwise.

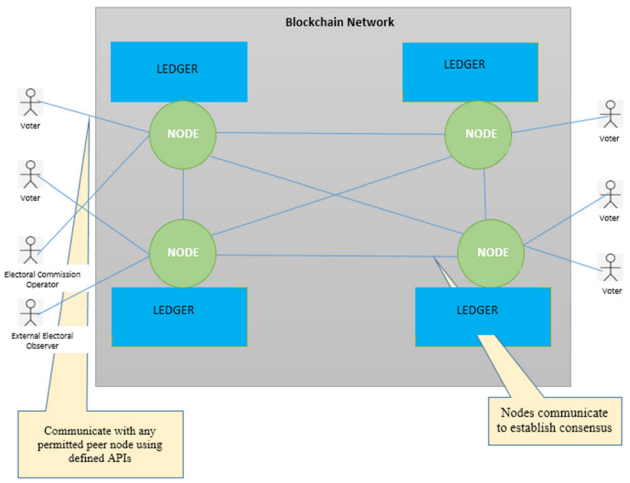

Fig. 6 Architecture of the proposed system

7 Conclusion and future work

In this paper, we addressed the common existing problems from the traditional voting systems amongst African Nations. Certainly, centralized architecture of the voting process used in the traditional system permits the involvement of corrupt practices and the invalidity of the entire voting process. The paper introduces the blockchain decentralized architecture that gives flexibility and adequate security to the entire process. Flexibility in term of voter access at convenient location and fully secure on the blockchain network layer.

The paper's goal was to expose a solution for a longtime existing unjust practices in electoral processes. The techniques proposed in this paper focus on minimizing the electoral rigging, discarding invalid votes, reduce violence in electoral polling units, minimize running cost of an electoral process in every electoral procedure over the entire globe.

There are some other relating issues facing electoral processes in some African Nations are not answered with the proposed system. Issue such as; Vote Buying. Such issue is a socio-economical problem and is difficult to trace and control.

References

1. Electoral Commission of Namibia (ECN) (2014) Online. Retrieved February 12, 2019 from https://www.ecn.na/wp-content/uploads/2019/07/Post-Election-Report-2014.pdf
2. Peters GW, Panayi E, Chapelle A (2015) Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective
3. Foroglou G, Tsilidou AL (2015) Further applications of the blockchain. In: 12th student conference on managerial science and technology
4. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the blockchain model of cryptography and privacypreserving smart contracts. In: Proceedings of IEEE symposium on security and privacy (SP), San Jose, pp 839–858
5. Akins BW, Chapman JL, Gordon JM (2013) A whole new world: income tax considerations of the bitcoin economy
6. Zhang Y, Wen J (2015) An iot electric business model based on the protocol of bitcoin. In: Proceedings of 18th international

conference on intelligence in next generation networks (ICIN), Paris, pp 184–191
7. Sharples M, Domingue J (2015) The blockchain and kudos: a distributed system for educational record, reputation and reward. In: Proceedings of 11th European conference on technology enhanced learning (EC-TEL 2015), Lyon, pp 490–496
8. Noyes C (2016) Bitav: fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405
9. Madavi D (2019) A comprehensive study on blockchain technology
10. Venkatapur RB, Prabhu B, Navya A, Roopini R, Sai Niranjan AS (2018) Electronic voting machine based on blockchain technology and aadhar verification. Int J Innov Eng Sci 3(3):2018
11. Alam M, Bokhari MU (2007) Information security policy architecture. In: ICCIMA'07: proceedings of the international conference on computational intelligence and multimedia applications (ICCIMA 2007), IEEE Computer Society, Washington, DC, pp 120–122
12. BlockchainHub (2018), "Smart Contracts". Online. Retrieved March 28, 2019 from https://blockchainhub.net/smart-contracts/