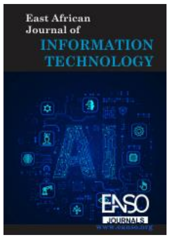


East African Journal of Information Technology
eajit.eanso.org
Volume 6, Issue 1, 2023
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EASO
EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Modernizing the Kenyan Electoral System through Polkadot Blockchain Network

Richard Kyalo Mutuku[1*]

[1] University of Nairobi P. O. Box 30197, 00100 Nairobi, Kenya
* Correspondance ORCID ID: https://orcid.org/0000-0003-0919-6022; Email: richardkyalo9@gmail.com

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

Date Published:

04 May 2023

Keywords:

Blockchain, Voter Fraud, Digital Democracy, Polkadot, e-voting

ABSTRACT

The 2007/8 post-election violence in Kenya brought the nascent Kenyan democracy to the brink of collapse. It anachronistically demonstrated that old ways of managing elections were being antiquated by new realities, such as a growing population, the need for technological support, and the immediacy of a supportive electoral legal regime. A decade and a half after the posthumous murder of Kenyans during the 2007 disputed election, Kenya is leapfrogging and sauntering to establish a vibrant democracy, albeit with specific challenges. Firstly, the presidential elections have been disputed thrice after the promulgation of the constitution in 2010. And secondly, the allegation of voter fraud against the electoral body is imminent. Further, public trust in the electoral body is low and has been so since the advent of pluralism politics in 1991. Besides, the electoral body gets overwhelmed by the number of elections they manage during the general elections, and technological failures have been a significant impediment. Ostensibly, these challenges compound an existing problem of mistrust among political players and gather moss, especially during the period between the end of the voting exercise and the announcement of presidential results by the electoral body. Erstwhile, such a fragile situation manifested and threatened public safety after the 2013, 2017, and 2022 general elections. However, despite scepticism, the finality of the supreme court process as an arbitrator of the disputed presidential elections has played a role in quelling violence and settling such matters. In this article, the author argues that the maturation of digital democracies and the incorporation of blockchain technologies can modernize grassroots elections and resolve allegations of voter fraud.

APA CITATION

Mutuku, R. K. (2023). Modernizing the Kenyan Electoral System through Polkadot Blockchain Network. *East African Journal of Information Technology*, *6*(1), 77-90. https://doi.org/10.37284/eajit.6.1.1199

CHICAGO CITATION

Mutuku, Richard Kyalo. 2023. "Modernizing the Kenyan Electoral System through Polkadot Blockchain Network". *East African Journal of Information Technology* 6 (1), 77-90. https://doi.org/10.37284/eajit.6.1.1199.

HARVARD CITATION

Mutuku, R. K. (2023) "Modernizing the Kenyan Electoral System through Polkadot Blockchain Network", *East African Journal of Information Technology*, 6(1), pp. 77-90. doi: 10.37284/eajit.6.1.1199.

IEEE CITATION

R. K. Mutuku, "Modernizing the Kenyan Electoral System through Polkadot Blockchain Network", *EAJIT*, vol. 6, no. 1, pp. 77-90, May. 2023.

MLA CITATION

Mutuku, Richard Kyalo. "Modernizing the Kenyan Electoral System through Polkadot Blockchain Network". *East African Journal of Education Studies*, Vol. 6, no. 1, May. 2023, pp. 77-90, doi:10.37284/eajit.6.1.1199.

INTRODUCTION

Voter fraud and a political environment undergirded by mistrust are the banes that hurt the Kenyan democracy. After the reintroduction of multiparty politics in 1992, heralded by the repeal of section 2A of the constitution, three things happened to the republic. Firstly, more political players joined the space, and secondly, the Kenyan republic started to enjoy a semblance of free speech. Further, civil participation in democratic processes and interest in governance among Kenyans soared. Nonetheless, whether real or contrived, one thing has remained a constant—voter fraud (Mebane, 2017). Allegations of electoral malpractices and unfairness emerge after every general election. In recent times, the massive deployment of technology, especially in the transmission of presidential results, has compounded the problem and, in certain instances, pushed the country to the cusp of fragility and savagery, as experienced in the 2007/8 post-election violence. Nonetheless, blockchain technology provides a prodigious solution to some of these challenges as it can make the transmission of election results immutable and verifiable. In this article, therefore, the writer derives the historical instances of voter fraud in Kenya and proposes a blockchain model that can provide greater transparency and verifiability of the electoral results. Besides, the author utilizes case studies from the successful deployment of blockchain technology globally to justify the proposed solutions.

History of Voter Fraud in Kenya after 1992

Kenya became a de-jure state or a one-party state in 1969 when the government banned Kenya's People's Union from organizing competitive politics. Later, in 1982, the National Assembly passed a constitutional amendment that formally declared Kenya a de-jure state. From 1969 to 1991, KANU orchestrated an autocratic regime undergirded by clientelism, human rights abuses, stifled democratic space, extra-judicial killings, state-sponsored violence, and detention of dissidents. At the turn of 1990, a wave of democratic pluralism swept across Africa, and Kenya was no exception. President Daniel Moi and his government received immense pressure from Western allies, international stakeholders such as the World Bank, and local civil society groups to pave the way for competitive politics, posthumously regarded as the clamour for the repeal of section 2A that allowed multiparty politics. When the President repealed section 2A in December 1991, it ushered in a new era of multiparty politics, and Kenya has not looked back (Long, 2008). However, with its tremendous benefits, multipartyism introduced new challenges in election management, sometimes morphing into regrettable events such as voter fraud and tribal violence as experienced in successive elections.

The election of 1992 heralded multiparty competition attracting eight political parties to the presidential contest. On December 29, 1992, the

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

election pitted KANU's strongman, President Moi, against seven other candidates. The voting process faced a ubiquity of election malpractices and institutional interferences. For instance, the polling stations opened late in some provinces, and the electoral commission failed to provide mobile polling stations as initially promised. These challenges affected the voting and tallying process as some centres continued voting the following day. Similarly, during the campaign period, the ruling party deployed state resources and used the provincial administration to intimidate competitors. Even though President Moi won the election, there have been diametrical views regarding whether the voting process was without fraud (Long, 2008).

In 1997, Kenyans approached the general elections amid a harsh economic environment orchestrated by the full effect of the structural adjustment programs and grand corruption during the Goldenberg era. As for the general elections, the number of registered political parties increased dramatically from eight in 1992 to 22 in 1997. The repeal of section 2A in 1991 shaped democratic plurality, but election malpractices and voter fraud sprawled with the rising competition. The elections happened on December 29 and continued up to December 30. Nonetheless, some of the challenges faced in the 1992 elections also manifested. Some polling stations in northeastern and Coast provinces opened late due to logistical challenges compounded by flash floods in the sub-regions. President Moi won the election by 40%, followed by Mwai Kibaki with 30%. The disorganization of the opposition candidates and the use of the police to block opposition candidates from campaigning gave KANU an upper hand in winning the election (Barkan & Ng'ethe, 1998).

The 2002 general election is widely considered a successful election with the hallmarks of fairness, transparency, and state non-interference. The Commonwealth Observer Group described the electoral process as credible and that the conditions favoured a free and fair election that reflected the will and aspirations of the people (Commonwealth Observer Group, 2013, p. 3). However, it must be noted that the constitution barred the incumbent President Moi from contesting the third time even though he had served five terms. Had he contested the peradventure, the outcomes would have been different. Secondly, the opposition had learned a lesson from the woeful failures of 1997 brought by disorganization, favouring President Moi's re-election (Society for International Development, 2015, p. 10). This time, the opposition united under the National Rainbow Coalition (NARC)—an amalgam of the National Alliance Party of Kenya and Raila Odinga's Liberal Democratic Party of Kenya. NARC faced KANU's Uhuru Kenyatta with the mantra "Yote Yawezekana Bila Moi." Mwai Kibaki of NARC had a 62.2% pyrrhic win against Uhuru Kenyatta's 30% national tally.

Fast forward to 2007, Kenya went to the general elections on December 27, 2007, pitting two leading contenders: Mwai Kibaki of the Party of National Unity (PNU) and Raila Odinga of the Orange Democratic Movement (ODM). The voting exercise was good; however, hell broke loose during the national tally of presidential results. By December 28, 2007, Raila Odinga enjoyed a comfortable lead against Mwai Kibaki. As a result, the ODM party declared Raila Odinga president-elect. However, as tallying continued, the gap between the two narrowed, and accusations of voter fraud began to emerge from the ODM side, calling Mwai Kibaki to concede defeat and order a recount. On December 30, 2007, the defunct Electoral Commission of Kenya, chaired by the late Samuel Kivuitu, declared Mwai Kibaki the winner with 4,579,034 against Raila Odinga's 4,352,860. Later that evening, Mwai Kibaki was sworn in as President at the State House. As these events unfolded, violence sprawled in enclaves domiciled by Kikuyu and Luo ethnic minorities, especially in Nairobi and Rift Valley provinces. By the end of January 2008, ethnic cleansing and sporadic violence had claimed 1,333

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

people and displaced at least 600,000 people in the two provinces.

The nation had not experienced such a level of animosity and ethnic-motivated bloodletting since the Mau Mau war. The international community, especially the African Union, played a significant role in resolving the conflict, leading to the grand coalition government spearheaded by the Late Kofi Anan. The Kriegler Commission, under the auspices of the Independent Review Commission, was formed to investigate the disputed election and provide recommendations for electoral reforms. Some of the Kriegler commission findings were that the two competing sides perpetrated electoral malpractices in their strongholds, which made it difficult to establish the winner of the election (Society for International Development, 2015, p. 49). The malpractices bordered issues of ballot stuffing, voter bribery, police intimidation, and ECK's incompetence in conducting a free and fair election.

The post-election violence of 2007/8 heralded a ubiquity of electoral reforms anchored in the constitution promulgated in 2010. Among them was the use of electronic technology to support voter registration and voting, leadership and integrity laws, and a new election legal regime (Society for International Development, 2015, p. 88). As Kenya went to the general elections on March 4, 2013, messages of peace and "never again" will the country go into civil and ethnic strife because political competition dominated the campaign period. However, fears and mistrust due to the massive deployment of electronic voting systems and flawed procurement procedures threatened the integrity of the vote. This time, the Independent Elections and Boundaries Commission was responsible for conducting elections under the new constitution. The electoral body would conduct unprecedented six elections on the same day, including presidential, parliamentary, and county elections. The exercise was largely peaceful on voting day, to the chagrin of many naysayers who predicted violence. However, underneath the veneer of peace experienced across the country, massive system failures of biometric voter identification kits (BVR) were happening, resulting in manual registers in most polling centres to verify legitimate voters.

The system failures also affected the national tallying of presidential results, and the IEBC had to fall back to the use of manual tallying systems. The announcement of presidential results was delayed for five days of counting amid rising tensions and messages of peace. On March 9, 2013, IEBC declared Uhuru Kenyatta president-elect after garnering 50.07% of the vote, trailed by Raila Odinga's 43.3% of the national tally. Raila Odinga challenged the results in the Supreme Court as the final arbiter of presidential election disputes. The dispute was thrown out based on evidentiary technicalities. Different stakeholders, such as the Election Observer Group (ELOG), pointed out glaring cases of electronic voter fraud and illegal use of the two parallel voter registers informally regarded as the "Green Book." The opposition leaders blatantly refused to recognize the new government's legitimacy despite saying they would respect the Supreme Court ruling for the sake of peace (Long, 2008).

As Kenya headed to the 2017 general elections, there were many lessons to learn from the 2013 disputed election. Firstly, electronic voting and transmission of results needed to be tamper-proof and verifiable, and secondly, a poisoned political environment bred mistrust and unbelievable results. The campaign period had episodes of police brutality, intimidation of independent institutions, and deep tribal overtones. Kenyans went to the election on August 8, 2017, to elect their preferred candidates. On the one hand, was Jubilee Party's Uhuru Kenyatta, and on the other hand Raila Odinga of National Super Alliance (NASA), among other candidates (The Carter Center, 2018, p. 4). The electronic voting and tallying process were largely successful, especially at the county-level

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

tallying centres. However, challenges began to emerge with the transmission of results, as there were unjustifiable delays and a lack of transparency at the national tallying centre handling the presidential votes. The morning after the voting day, the IEBC started streaming provisional results on their official website, and President Kenyatta had an incessant lead of 10% ahead of his nemesis Raila Odinga. NASA and Raila Odinga began to raise concerns regarding massive electronic rigging propelled through hacking activities that multiplied Uhuru's votes through a scalar constant.

On August 11, 2017, the IEBC hastily announced the presidential results before receiving and collating results from all the polling stations. That haste decision raised political overtones as the body denied election observers and party representatives access to polling station results to verify and cross-check with parallel tallying such as one conducted by ELOG and media houses. The IEBC declared Uhuru Kenyatta the winner after garnering 54% of the national tally against Raila Odinga's 45% (The Carter Center, 2018, p. 5). The latter challenged the results at the Supreme Court, and on September 1, 2017, they were nullified for lacking simplicity, verifiability, and transparency, which are fundamental constitutional maxims for Kenyan elections. The IEBC declined to "open the servers" for opposition experts and interest groups to verify the veracity of the results. The Supreme Court called for another election within 60 days; however, the opposition boycotted, giving Uhuru Kenyatta an easy win, albeit with legitimacy questions.

The Problem

Old tricks die hard. Elections in Kenya still face the same old challenges and a vicious cycle of voter fraud, bribery, and ethnic mobilization. Since the multiparty elections in 1992, all except the 2002 general election lacked the objects of transparency, verifiability, and auditability. 2013, 2017, and 2022 elections had the highest deployment of electronic technology and monitoring through social media and media coverage but still did not pass the test of verifiability and transparency. The centralized electoral bodies lack mundane independence and have little or no safeguards against political interference and their own election regulations enforceability. Besides, the blatant refusal by IEBC to open the servers in 2017 to allow independent verification of election results pointed to the dangers of centralization of electoral management and institutional incompetence in promoting transparency, auditability, and verifiability of election outcomes. In the August 2022 general election, the IEBC deployed massive technology for identifying, verifying, and transmitting presidential results to the national tallying centre from grassroots polling stations across the country.

However, such technological rigour did not cure the two banes that hurt Kenya's election results management—verifiability and public trust. Allegations of cyber hacking and electronic manipulation of results during transmission emerged, creating a vicious legal animadversion at the Supreme Court of Kenya. Raila Odinga, the main nemesis against President William Ruto, did not prove the claims of cyber hacking and electronic manipulation of results during transmission. However, despite the court settlement, the verifiability, immutability, veracity, and public trust of the election results remain a lingering question (Juma & Oguk, 2020). These challenges point to systemic weaknesses of the centralized electronic management system and a poisoned culture of mistrust that vitiates the budding Kenyan democracy. In this article, the author proposes a piecemeal adoption of blockchain technologies to resolve the vicious cycle of voter fraud in Kenyan elections.

DIGITAL DEMOCRACY AND E-VOTING SUPPORTED BY BLOCKCHAIN TECHNOLOGY

Kenya's 2013, 2017, and 2022 general elections had a massive internet, electronic, and social media

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

deployment. Some venerated political scholars, such as Nanjala Nyabola in the book *Digital Democracy, Analogue Politics*, have termed this technology deployment as an enabler to democratic practices such as general elections, essential for electing and legitimizing leadership. Nyabola, in this book, cautions that technology deployment does not necessarily equate to a utopian democracy but rather an ancillary tool for making the processes seamless (Nyabola, 2018). In suggesting the centrality of blockchain technology in smoothing election malpractices in Kenya, the author is not dystopic about the use of technology. Rather, there is a recognition that any useful technology is as good as the users and the environment in which it is deployed to solve a problem. For instance, an environment of mistrust breeds chaos, and regardless of the robustness of the technology, the believability of the outcomes would be questionable. Therefore, even when this article suggests a phased deployment of blockchain technology, there is a realization that this may not necessarily be a masterstroke in resolving all the election malpractices and the public distrust of the electoral body.

Blockchain technology provides substantial opportunities for disrupting electronic voting and transmission of results in Kenya and across the African continent to deal with the existential threats of lack of transparency and verifiability. Electronic voting has gained traction in mature democracies such as the United States and Europe but is yet to gain a foothold in the African continent for the apparent reason: distrust. Electronic voting allows voters to cast their votes online by accessing an official electoral portal supported by internet connectivity. It eliminates the necessity for printing ballot papers, managing an election, and reducing voter apathy associated with voter intimidation and bribery. Despite these benefits, electronic voting and voter identification using BVR kits face particular vulnerabilities, such as those experienced in Kenya's 2013, 2017, and 2022 general elections. Those vulnerabilities include the possibility of hacking the centralized election management system, as was alleged in the 2017 and 2022 general elections, and denial of service due to system failures, as happened with the Electronic Voter Identification (EVID) kits in the 2013 general elections (Marwa, 2022). The incorporation of technology in the 2013 and 2017 general elections aimed to address some of these challenges by providing an accurate, transparent, legitimate, and verifiable election outcome. However, vicious disputes arise every other election. Those disputes culminated in the cancellation of presidential results in 2017 by the Supreme Court due to irregularities and illegalities during the entire transmission of the results exercise (Marwa, 2022).

Blockchain technology can address some of the challenges associated with tallying, transmission, and verifiability of results. Jafar et al. (2021) described that blockchain embodies a decentralized technology using distributed ledger technologies with end-to-end encryption for advanced protection and non-repudiation. These blockchains, made of blocks or loosely translated as files, are a growing list of files with cryptographic interconnectedness. All the blocks or files have a timestamp, hashes, and transactional history of past activities. The Bitcoin blockchain is the pioneer blockchain, and others, such as Ethereum, Ripple, and Polkadot chains, have emerged. The initial idea behind blockchain technology was to provide data protection and leverage transparency, verifiability, and non-repudiation.

In the context of electronic voting, an eligible voter gets to cast a vote through an online portal anonymously. The vote is protected through tamper-proof and encrypted keys though the ledger is public, and anyone can access the data without necessarily knowing the voter's personal information. The beauty of blockchain technology is that the public ledger provides a permanent and immutable record such that nefarious and malicious hackers cannot tamper with the record. However,

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

even when malicious individuals tamper with the votes, the peer-to-peer network ensures that the original record is traceable (Jafar et al., 2021). Therefore, one would have to hack all the blocks or files to compromise the votes successfully, which is nearly impossible. The ability to audit blockchain records through shared computer ledgers and peer-to-peer networks makes it impossible to tamper with or impose fraudulent votes such as ballot stuffing, double entries, or multiplication of results through a constant. In other words, blockchain technology ensures that observers and voters themselves can trail the votes and any changes made during the tallying process to improve verification and transparency because the records are publicly accessible.

METHODOLOGY

The researcher utilizes case study methodology to conduct an in-depth analysis regarding the applicability of blockchain technology in resolving voter fraud in Kenya. The study examines the historical voter injustices in Kenya since the beginning of multipartyism and derives real-world examples of voter fraud by citing publicly available information. Further, the study examined real-world applications of blockchain technologies worldwide involving the use of blockchain to conduct elections and the benefits accrued from such ventures, from which Kenya can draw a lesson. Finally, the researcher examines the feasibility of implementing blockchain technologies based on their scalability, effect on climate change, transaction costs, and mass adoption.

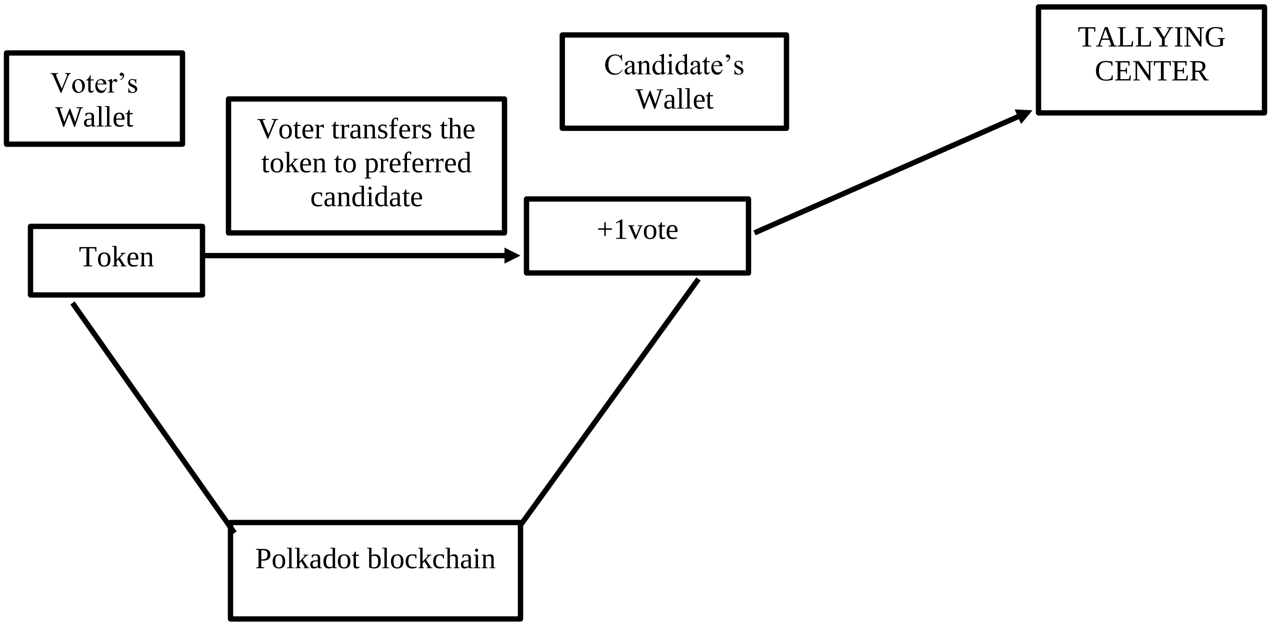
Proposed Polkadot Blockchain to Support Electronic Voting in Kenya

This research proposes that the full maturation of the Polkadot blockchain will be able to handle huge transactions involved in a general election due to its scalability. Notably, scalability allows a blockchain network to handle big blocks of transactions, perhaps in millions, without depleting its resources or imposing higher transaction fees and electricity costs. The full scale of the Polkadot blockchain will be able to handle 1 million transactions per second, which is massive compared to its antecedents. For instance, the bitcoin blockchain has an extremely low scalability of 4.6 transactions per second, while the Ethereum blockchain can only handle 15 per second (Steinbrenner, 2022). Therefore, the scalability of the Polkadot blockchain with para-chains and para-threads will help overcome the substantial gas fees involved in the Ethereum network, the high electricity required by the bitcoin blockchain to confirm transactions, and fewer transactions per second supported by the two legacy blockchains.

It is proposed that the electoral body will require to set up an electronic voting platform on the Polkadot network. An eligible voter will have an account or a "wallet" on the portal and be issued six tokens or coins (read as ballot papers), each representing an opportunity to vote. In the Kenyan context, a voter must vote for six candidates in the different categories: President, governor, senator, woman representative, member of national assembly, and member of the county assembly. In all the categories, the voter can only vote once by transferring the token from their wallet to the preferred candidate's wallet (interpreted as the ballot box). For instance, in the presidential category, the voter can only vote for one candidate among many by transferring the token from their wallet to the preferred candidate's wallet. Once a vote is cast, no other changes can be made after the election period. Voters can only change their vote for other candidates during the official voting period. The process repeats for all other categories of candidates. In this hybridized model, the electoral body is responsible for collating and declaring the winners in the different elective posts.

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

Figure 1: Demonstrates proposed voting system supported by Polkadot blockchain



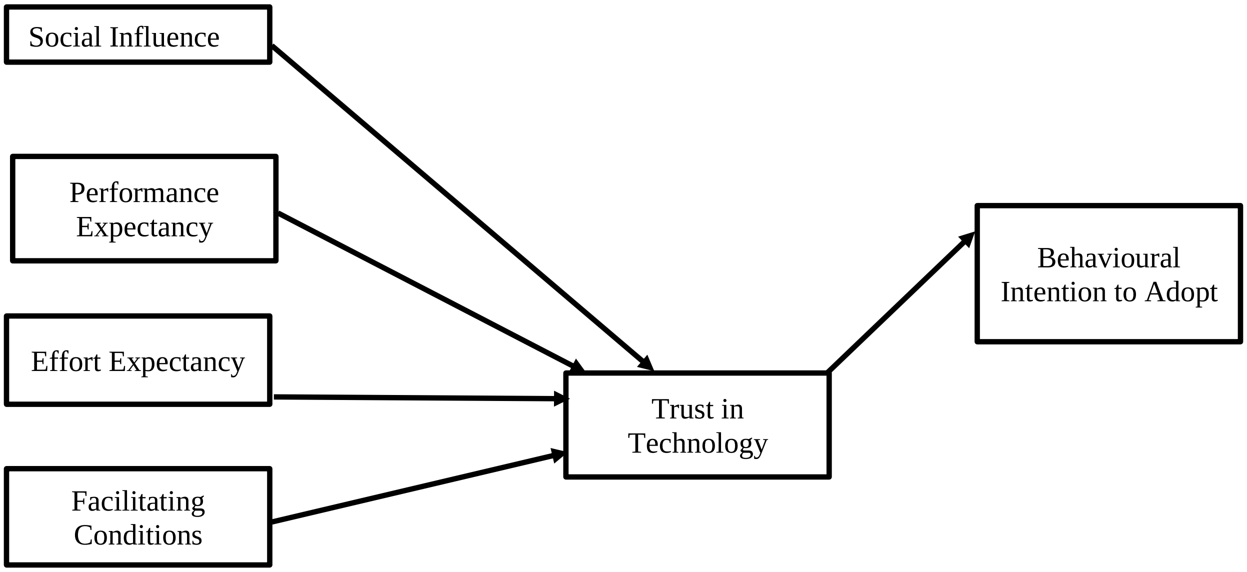
The Polkadot blockchain makes it easier to confirm transactions almost in real-time to avoid delays that have previously affected the transmission of results in Kenya. Secondly, the speed also provides a robust ecosystem for verifying results in millions of transactions, which would take forever in Ethereum or Bitcoin networks. Contextually, this proposed technology is implemented in lower cadre elections before a mass election like the presidential election. The country can begin utilizing it in managing party nominations, by-elections, and member of county assembly elections as they do not involve massive data flows and political sensitivities.

Theoretical Underpinnings: Unified Theory of Acceptance and Use of Technology (UTAUT) Model

The UTAUT model originated from the seminal works of Venkatesh et al. (2003). The scholars harmonized the findings of eight subsequent empirical studies and developed four primary constructs in the unified model to explain behavioural intention to use technology. These constructs include Social Influence (SI), Performance Expectancy (PE), Effort Expectancy (EE), and Facilitating Conditions (FC). The original model had other mediating variables such as age, gender, experience, and voluntary use. Nonetheless, modern theorists no longer use those moderators as their adherence and efficiency diminish with the context (Wamba & Queiroz, 2019). Ostensibly, this study does not include moderating variables; however, it introduces trust as the intervening variable.

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

Figure 2: Proposed UTUAT Model



Source: (Hybridized from Venkatesh et al. (2003) and (Wamba & Queiroz, 2019))

Social Influence (SI)

Venkatesh et al. (2003) defined social influence as the degree to which a user perceives that significant others believe they should use the new technology (p. 451). Significant others include family, peers, and friends. They can exert pressure on an individual to adopt and use blockchain technology. For Francisco and Swanson (2018), blockchain technologies are social technologies; therefore, normative pressure can cause massive adoption (p. 7). Therefore, mass intention to use blockchain technology, especially among the youth, can lead to extensive behavioural intention for adoption. In retrospect, the empirical studies of Wamba & Queiroz (2019) and Francisco and Swanson (2018) have found a positive relationship between social influence and behavioural acceptance of blockchain technologies. Therefore, to support the adoption of the proposed use of Polkadot blockchain technology, policymakers must use tools such as social media to promote the technology for mass adoption, primarily among the youth.

Performance Expectancy (PE)

PE embodies the degree to which users believe technology will provide the expected benefits (Francisco and Swanson, 2018:6). In other words, Yusof et al. (2018) noted that PE is the perception that using technology will yield expected gains (p. 276). Contextually, Kenyans will adopt blockchain technologies in electoral systems if they believe it will fight voter fraud and increase transparency and verifiability of results. Khazaei (2020), Francisco and Swanson (2018), and Wamba & Queiroz (2019) confirmed that performance expectancy was a strong predictor of behavioural intention to adopt new technologies.

Effort Expectancy (EE)

EE refers to the ease of use of technology. If users perceive technology as complex and challenging to use, they are less likely to adopt it (Yusof et al., 2018: 276). Therefore, blockchain technologies involved in electoral systems must be simplistic and provide a more seamless user experience than the existing technologies. Ostensibly, these technologies must accommodate older voters,

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

persons with disabilities, the digital divide, and voters with limited technical know-how. As such, voter education and public simulations are critical in Kenya before the actual voting exercise to minimize public mistrust and promote seamless use. Otherwise, many voters are likely to avoid using the technology if they perceive difficulties in use. Empirically, Yusof et al. (2018) found a positive linkage between effort expectancy and mass adoption of blockchain technologies (p. 276).

Facilitating Conditions

Venkatesh et al. (2003) explained facilitating conditions as the magnitude with which users perceive that organizational and technical infrastructure is available to support the usability of new technology (p. 451). Blockchain technology is highly networked and requires technical and organizational resources to support its operation. The absence of these ancillary resources is likely to influence its use adversely. Wamba & Queiroz (2019) explained that the facilitating conditions include internet connectivity, cloud-based technologies, internet-enabled gadgets, power supply, and communication equipment (p. 1717). In Kenya, the digital divide is wide. For instance, according to Mariwa (2019), the 3G internet penetration is at 90%. However, only 70% of Kenya has 4G network connectivity, supporting the current electronic voting system. In the 2013 general election, the power supply hampered voter identification and transmission of results. Many Electronic Voter Identification System (EVID) gadgets had not been charged fully and lost power midway through the voting day. These challenges —internet connectivity and power supply, especially in rural areas—can impede the acceptance of the proposed Polkadot blockchain technology in managing election results. This relationship is established in the works of Wamba & Queiroz (2019), Yusof et al. (2018), and Francisco and Swanson (2018).

Trust in Technology

The Kenyan political space is wrought with mistrust among the players, institutions, and technologies deployed. There is a tendency to bastardize the electoral body and accuse it of colluding with competitors to rig elections. Opposing sides incessantly accuse each other of engaging in voter fraud, especially in their strongholds. Likewise, it is common for political players to allege hacking and electronic manipulation of results to favour the other side. Such an environment of mistrust breeds a lack of believability in new technologies and erodes public trust and credibility of election results. Tseng and Fogg (1999) have argued that technology's credibility influences people's perceptions and attitudes and consequently affects the adoption decision (p. 40). In this regard, users may show reticence or hesitance in adopting blockchain technologies if they perceive them as insecure, malleable, and lacking verifiability. Even though blockchain technology has characteristics of verifiability and immutability, a poisoned political environment can render it useless. Bipartisan consensus and trust are necessary for Kenya before deploying blockchain technology. Regardless of the benefits, the political class must behaviourally accept it first and cascade the trust to the public.

Use Cases of Blockchain Technology in Electoral Processes Globally

Thailand, in 2018 became the first country to implement the use of blockchain technology in conducting party primaries. The Thailand Democratic Party used the Zcoin blockchain technology to conduct party primaries involving 120,000 party members. The election was a success, leading to the election of Abhisit Vejjajiva as the party flag bearer in a transparent and verifiable manner. Party members voted using a mobile app by submitting their photo ID, and Rasberry Pi-based network would verify the votes and confirm them using a peer-to-peer distributed ledger (Tan, 2018).

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

Similarly, in 2018, Sierra Leone became the first African country to use blockchain technology on a massive scale to conduct an election on a national scale. The nation used Agora's blockchain to run parallel voting and tally election results by storing all announced results from the polling stations on a private blockchain and posting the results online. The exercise reduced instances of voter fraud common in many African elections and validated results in real-time without the possibility of manipulation. In essence, the Agora ecosystem encourages voters and candidates to participate in an election devoid of manipulation and lack of transparency (Perper, 2018).

Further, in 2021, West Virginia state used the Voatz blockchain ecosystem to conduct a trial run for federal military elections. Voters were required to verify their voting eligibility by providing their identity, image, and biometrics through retinal scans and fingerprints. A mobile app designed by Voatz conducted those verifications in real-time by cross-checking the provided photo ID with those provided by the voter before allowing them to vote. The application and blockchain technology eliminated double voting, identity theft, and possible election fraud (Nguyen, 2018).

Opportunities and Challenges Emerging from the Use of Blockchain Technology in Election Management

While blockchain technologies provide an immense capability for resolving election malpractices, it is necessary to recognize that the technology is nascent and requires extensive research and innovation for its maturation. Blockchain technologies became popular after the emergence of the bitcoin cryptocurrency. Notably, blockchain technologies are undergirded by open-source codes, decentralized ledgers, and distributed databases that store transactional data. These novel technologies do not rely on centralized intermediaries such as electoral bodies or banking systems (Francisco & Swanson, 2018). Instead, they allow users to transact directly using interconnected and duplicatable ledgers called blockchains. Blockchains provide immutable transparency compared to centralized systems because transactions do not require third-party confirmation but rather network consensus.

According to Kshetri and Voas (2018), blockchain technology provides ample opportunity for countries with a history of election fraud to resolve voter tampering and malpractices. Accordingly, blockchain offers a cryptographic method for securing voting records by establishing an accurate, secure, transparent, and immutable record of transactions for election verifiability. In this regard, no state organ or entity can manipulate or modify the results without tampering with all the blocks or files, which is nearly impossible. However, even when these benefits are palpable, blockchain technologies suffer the challenge of scalability and depletion of resources. Blockchain technologies are efficacious in small-scale assignments, according to Jafar et al. (2021). Large-scale operations such as nationwide elections can overwhelm the ecosystem, leading to inordinate cost overruns, time lags due to confirmations, and sometimes denial of service attacks. A national election in Kenya would involve more than 10 million voters; therefore, the number of nodes in the blockchain ecosystem would also be substantial, requiring scaling of the network. Currently, the Bitcoin, Binance Smart chain and Ethereum networks cannot support many transactions without overstretching the ecosystem. That requires the use of parallel nodes or sidechains to support data concurrency. Otherwise, the Polkadot blockchain needs urgent completion to effectively support such transactions per minute.

Blockchain technologies also guarantee voters' anonymity and vote secrecy, a fundamental maxim of democracy. Voters prefer to exercise their free will without intimidation from the state or third parties for making choices one way or another. While that is the case with blockchain technologies, using pseudonyms cannot guarantee total privacy

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

for voters. The transactions are public for scrutiny; therefore, a close introspection of data may reveal the real identities of voters. As such, some critics have argued that blockchain technologies may not be suitable for nationwide elections, mainly because data privacy might be at risk in exchange for transparency and openness (Kshetri and Voas, 2018).

Further, blockchain can help address voter apathy and logistic problems that bar many eligible voters from participating in democratic activities. With blockchain, voters can vote online, provided they have internet access. However, the overarching challenge hinges on the acceptability of this technology and resistance to change among the political class. Undoubtedly, blockchain technology is the panacea to opaqueness in the electoral process, but its intricacy is the greatest bane that may derail its acceptability. Many voters and political leaders in Kenya have a limited understanding of blockchain technology. For that reason, they are less likely to support such a disruptive technology due to performance and effort expectancy (Francisco & Swanson, 2018).

Finally, climate change crusaders have legitimate concerns regarding the contributions of crypto and blockchain technologies to green gas emissions. Ostensibly, blockchain technologies utilize high amounts of energy, mainly in transaction confirmations, encryption, peer communications, and enabling protocols. Similarly, crypto mining of coins and tokens, the likely currencies in blockchain transactions, requires substantial energy and such power often does not come from renewable sources. Climate change proponents have concerns that using non-renewable sources of energy to support mining and blockchain activities contributes to the release of greenhouse emissions and depletion of the ozone layer, which contributes to the greenhouse effects. Such concerns are slowing down the mainstream adoption of blockchain technology, and many governments are tightening regulations to control pollution (Egiyi & Ofoegbu, 2020).

CONCLUSION

Kenya has a longstanding history of voter fraud and disputed presidential elections since 1991. The culmination of these disputes led to the heinous murder of Kenyans during the 2007/8 general elections. Since then, there have been successive legal and technical reforms in the electoral management and transmission of results to avert violence and electioneering crises. Nonetheless, these reforms have not solved the mistrust of political players against the electoral body and the lack of verifiability of election results. This article established that the innovation around the Polkadot blockchain could increase the verifiability, transparency, and trust of election results if integrated into the election management system. Blockchain technologies are distributed ledgers that store and verify transactional data without needing third-party confirmation. Therefore, a country like Kenya, with a history of voter fraud, can utilize blockchain and cryptographic methods to secure voting records as they provide accurate, verifiable, immutable, and transparent election results. However, it is critical to mention that large-scale operations such as national elections can overwhelm blockchains. Therefore, piecemeal use of blockchains as they undergo maturation is necessary, especially in less competitive elections such as party primaries and by-elections.

REFERENCES

Barkan, J. D., & Ng'ethe, N. (1998). African Ambiguities: Kenya Tries Again. *Journal of Democracy*, *9*(2), 32-48.

Commonwealth Observer Group, (2013). Report of the Commonwealth Observer Group: Kenya General Elections. https://thecommonwealth.org/sites/default/files/news-items/documents/130411.pdf

Egiyi, M. A., & Ofoegbu, G. N. (2020). Cryptocurrency and climate change: An overview. *International Journal of Mechanical*

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

Engineering and Technology (IJMET), *11*(3), 15-22.

Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1), 2.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, *21*(17), 1-22.

Juma, J., & Oguk, C. O. (2020). Election results' verification in e-voting systems in Kenya: a review.

Khazaei, H. (2020). Integrating cognitive antecedents to the UTAUT model to explain the adoption of blockchain technology among Malaysian SMEs. *JOIV: International Journal on Informatics Visualization*, *4*(2), 85-90.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *Ieee Software*, *35*(4), 95-99.

Long, J. D. (2008). Electoral fraud and the erosion of democratic gains in Kenya. Working Group in African Political Economy (WGAPE) Paper prepared for the Working Group in African Political Economy (WGAPE), 1-45.

Mariwa, F. (2019). Internet access: How rural Kenya is keeping pace. https://www.dw.com/en/internet-access-how-rural-kenya-is-keeping-pace/a-47071209

Marwa, R. (2022). The Competence of the Electoral Commission to conduct Free and Fair Elections in Tanzania: A Legal Analysis. *J. Pol. & L.*, *15*, 54.

Mebane Jr, W. R. (2017). Anomalies and frauds (?) in the Kenya 2017 presidential election. Working paper.

Nguyen, T. (2018). West Virginia to offer mobile blockchain voting app for overseas voters in November election. https://www.washingtonpost.com/technology/2018/08/10/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election/

Nyabola, N. (2018). Digital democracy, analogue politics: How the Internet era is transforming politics in Kenya. Zed Books Ltd.

Perper, R. (2018). Sierra Leone just became the first country in the world to use blockchain during an election. https://www.businessinsider.com/sierra-leone-blockchain-elections-2018-3?r=US&IR=T

Society for International Development, (2015). New Constitution, Same Old Challenges: Reflections on Kenya's 2013 General Elections. https://uraia.or.ke/wp-content/uploads/2016/12/SIDElectionsBook2013.pdf

Steinbrenner, M., (2022). Blockchain & Sustainability. https://neosfer.de/en/blockchain-sustainability/

Tan, A., (2018). Thailand’s Democrat Party holds election with blockchain. https://www.computerweekly.com/news/252452435/Thailands-Democrat-Party-holds-election-with-blockchain

The Carter Center, (2018). Kenya 2017 General and Presidential Elections. https://reliefweb.int/sites/reliefweb.int/files/resources/kenya-2017-final-election-report_0.pdf

Tseng, S. & Fogg, B.J. (1999). Credibility and Computing Technology. *Commun*. ACM 1999, 42, 39–44

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of

Article DOI: https://doi.org/10.37284/eajit.6.1.1199

information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Wamba, S. F., & Queiroz, M. M. (2019). The role of social influence in blockchain adoption: The Brazilian supply chain case. *IFAC-PapersOnLine*, *52*(13), 1715-1720.

Yusof, H., Munir, M. F. M. B., Zolkaply, Z., Jing, C. L., Hao, C. Y., Ying, D. S., ... & Leong, T. K. (2018). Behavioural intention to adopt blockchain technology: Viewpoint of the banking institutions in Malaysia. *International Journal of Advanced Scientific Research and Management*, *3*(10), 274-279.

