Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria

Temidayo Peter Abayomi-Zannu, Isaac Odun-Ayo, Barka Fori Tatama and Sanjay Misra

Abstract The voting system in Nigeria has always been filled with different forms of manipulation, and m-voting was suggested as the solution but has a major problem which is securely storing the casted votes. Blockchain was proposed to mitigate this problem and with the utilization of two-factor authentication to prevent illegible voters from casting their votes. The objective of this paper is to develop a mobile voting system that utilizes two-factor authentication to authenticate the voters and blockchain technology to securely store the votes. The system was then evaluated using the ISO 9241-11 usability model, and the results showed that the proposed system had a good usability rating which implies that it can be utilized in a voting procedure.

Keywords Blockchain · Mobile devices · Mobile voting · Two-factor authentication

1 Introduction

Voting is a process whereby an individual or group of individuals expresses their opinions or choices which can be either for or against a person (candidate) that could be either political (elections) and social or public [1]. Ballot/Paper voting is the most popular means of voting and is still being used in multiple countries around the world. Ballot voting is a type of voting procedure whereby the choices made by the voters must be kept secret. Voters tick out their preferred candidate on a piece of paper at

T. P. Abayomi-Zannu · I. Odun-Ayo · B. F. Tatama · S. Misra (✉)
Covenant University, Ota, Nigeria
e-mail: sanjay.misra@covenantuniversity.edu.ng

T. P. Abayomi-Zannu
e-mail: temidayo.abayomi-zannu@stu.cu.edu.ng

I. Odun-Ayo
e-mail: isaac.odun-ayo@covenantuniversity.edu.ng

B. F. Tatama
e-mail: barka.tatama@stu.cu.edu.ng

P. K. Singh et al. (eds.), *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*, Lecture Notes in Networks and Systems 121, https://doi.org/10.1007/978-981-15-3369-3_63

the polling station and then drops or submit them into the ballot box provided. This process is usually the standard method still being practiced in Nigeria and is often at times inaccurate, tedious, and risky [2]. Occasionally, the last tally or vote count can be altered, and this manual procedure is susceptible to political dishonesty, political fraud, and errors [3]. Sometimes citizens do not want to take part in elections due to multiple reasons such as the requirement to wait in line to cast their votes which can be over an hour or more which is very time-consuming, inability to visit the polling station where their registration took place due to their jobs or change in their place of residence, inadequate ballots papers, political intimidation, voters can be coerced to cast their votes for candidate's that is not their choice, rigging of the votes, and brazen falsification of the results [4, 5].

This has led to the introduction of m-voting (mobile voting) which is a subset of electronic voting as a means to mitigate this problem [6]. With m-voting, voters only require a mobile device which has been the most adopted means of communication and an Internet connection to take part in the electoral procedure [7]. One of the most problematic phases in m-voting is the managing of the votes which is the process of ensuring that casted votes cannot be altered or tampered with [8]. A centralized database was utilized to store the votes but is susceptible to DDoS attacks, and since it is being managed by an administrator, the stored votes could be changed, manipulated, or tampered with by the admin or a malicious insider [9]. Blockchain technology was proposed as a means to mitigate this problem which is a distributed ledger that manages an ever-increasing list of records protected from any form of revision or tampering [10]. It is decentralized so as to avoid a single point of failure with the group working together to confirm genuine transactions [11, 12]. Blockchain can be utilized as a database that can be used to record anything of value such as marriage licenses, deed, titles of ownership, and votes and is almost impossible to reverse [13].

Since mobile devices do not have enough resources to be a miner/node on the blockchain network, another means was needed for mobile devices to be able to send their transaction or votes to the blockchain pool to be stored [14]. In order for their transactions to be sent, they have to be eligible to do so, and one of the means of verifying their eligibility is through the use of authentication [15, 16]. Authentication is the process of proving who you claim to be which usually requires a mechanism for identification that can verify one's identity prior to granting them access, and multiple means of authentication is far better than a single means [17]. Mobile voting is often seen as a tool for building trust in electoral management, increasing the overall efficiency of the electoral process, advancing democracy, and adding credibility to election results [18]. With the addition of blockchain technology and two-factor authentication to m-voting, a secured and transparent voting system can be created which mitigate the major problems associated with the ballot/paper voting process still being utilized in Nigeria.

The focus of this paper is to develop a mobile voting system that makes use of blockchain technology and two-factor authentication to provide a secured mobile voting system that can be used in Nigeria. The study is structured as follows: Sect. 2

presents the related works; Sect. 3 shows the methodology; Sect. 4 provides the results and discussion; while Sect. 5 concludes the paper.

2 Related Works

Different methodologies were being applied to the voting sector in order to not only simplify the voting process but also protect the votes while avoiding any form of tampering or manipulation. This section looks at some of the ways different authors have tried to accomplish this. It was stated that an e-voting system must be fully transparent, secured, mitigate duplicated votes, and protect the attendee's privacy [19]. They were able to achieve this by designing a secured e-voting system that made use of blockchain technology. A network security mechanism for voting systems based on blockchain technology was created by Wu and Yang [20] which utilized the distributed architecture of a blockchain to increase the security aspect in the voting procedure and only allow the addition of data while negating any form of modifications. Sakinah et al. [21] proposed an electronic voting system application that utilizes blockchain technology as a secured decentralized database that could keep a record of the votes cast by eligible voters. They created a virtual voting custom currency called Kinakoin with which a user uses to cast their votes in the form of a coin from their wallet to the wallets of the candidates. This exchange was then affirmed through a procedure of mining, and the information of the exchanges was kept in the blockchain with a special hash which served as the square's unique fingerprint. Purandare et al. [22] noted that voting is an important aspect for democratic countries, and elections decide the future of that country; therefore, the tools/devices being used for the election process should be as transparent as possible while also having a high level of security. They designed an application that can be used for the voting process which voters can use on their Android smart phones. They also made use of one-time password (OTP) as a form of authentication to verify a voter's eligibility to vote and also prevent voters from casting their votes twice. Kshetri and Voas [23] mentioned that blockchains can solve two of the major or prevalent problems in the voting procedure which are voter access and fraud. They proposed a blockchain-enabled e-voting system that gives every voter a wallet and a single coin which is used to vote. An m-voting system was designed by Gajabe [24] that enables eligible citizens to cast their votes using their mobile devices and increases voter's participation in the electoral process. The voters are first authenticated to verify their eligibility to vote, and after the verification process, they are then granted access to cast their votes which is encrypted and then sent to the central server to be stored in the database which tallies the votes and shows the results. Most authors focused on utilizing blockchain technology in terms of cryptocurrency, but our focus is on making use of blockchain technology as a database to securely store the casted votes while avoiding any form of modifications. Also, we are making use of a two-factor authentication approach as a secured means of authenticating the voters to prove their eligibility and grant them access to cast their votes, while also preventing them from casting multiple votes.

3 Methodology

This section presents the existing system, the proposed system, design analysis, voter's activity diagram, blockchain's proof-of-work algorithm, pseudocode for the two-factor authentication sequence, and implementation screenshots.

3.1 Existing System

Ballot/Paper voting is the most popular means of voting and is still being used in many countries, especially in Nigeria [2]. Each voter would have to visit the polling station where their registration took place. They would then cast their vote by placing a mark or their fingerprint dipped in ink beside their preferred candidate and then proceed to place it in the ballot box. Once the voting process is completed, officials will then count the votes manually and tally the results (there may be a need for a recount in some case). These procedures are often inaccurate, risky, and dreary, and the results are susceptible to tampering or modifications. This manual procedure leaves room for blunders, political untrustworthiness, and political extortion [25].

3.2 Proposed System

The m-voting system would make use of blockchain technology as a database to safely store the casted votes mitigating any form of tampering and two-factor authentication to verify a voter's eligibility to cast their votes, thereby making sure that only eligible voters can cast their ballot. For the two-factor authentication, voter's identification number (VIN), personal identification number (PIN), and one-time password (OTP) would be utilized.

The system architecture is based on a three-tiered layered architecture which is made up of the presentation layer, logic/business layer, and the data layer, all having their roles in the total functionality of the system. Figure 1 presents the three-tier showing the different tiers.

- Presentation Tier: The presentation tier is where the voting application runs. It provides an interface for voters to interact with the voting system using their smart phones. From this layer, the user can log in and cast their votes which will be processed at the logic tier and stored at the data tier.
- Logic Tier: The system functionalities are carried out here and it is regarded as the most important layer. It is made up of the system service, middleware layer, and application services. The application is developed using Android Studio IDE, XM, Java, Ethereum Virtual Machine (EVM), Python, C++, and SHA 256.
- Data Tier: The data tier contains all the knowledge sources required to provide the needed voter's information and also store their casted votes. It consists of two

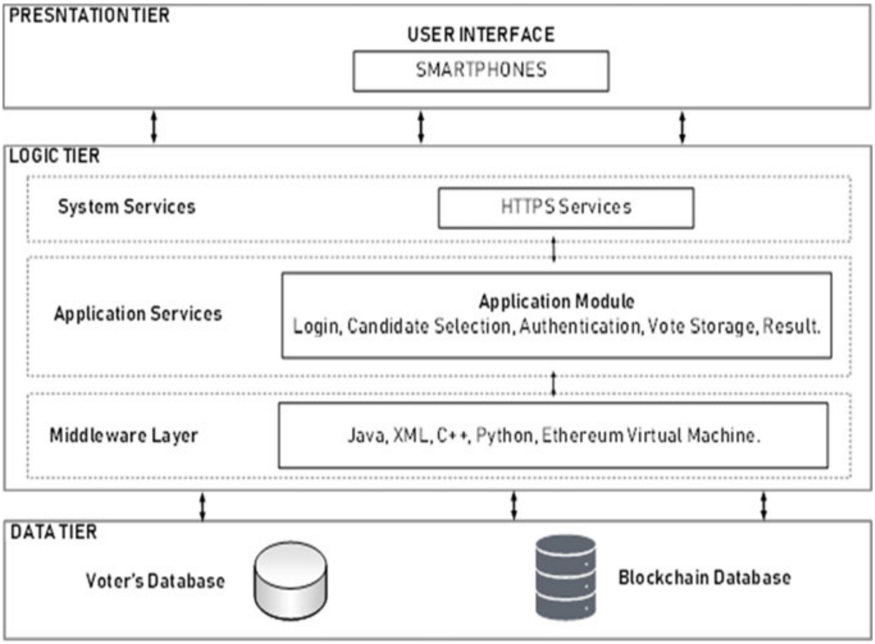


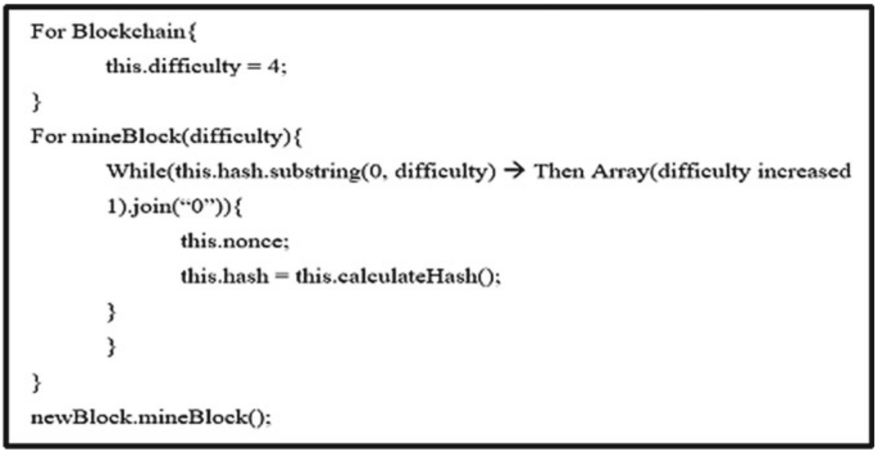
Fig. 1 m-voting architecture

(2) separate databases. The first database which is the voter's database contains every registered information about the voter which is used to identify each voter connecting to the system, and the second database which is the blockchain database is used to securely store the casted votes.

3.3 Design Analysis

In the design for this study, the most important requirements of the system were described below:

- Authentication of voters before access is granted to the application using their unique VIN and PIN.
- Enabling voters to select their preferred candidate.
- Authentication of voters before their vote is cast using the OTP.
- Storing and hashing of the casted votes in the blockchain database.
- Results can be viewed by everyone after the voting period.



```
For Blockchain{
        this.difficulty = 4;
}
For mineBlock(difficulty){
        While(this.hash.substring(0, difficulty) → Then Array(difficulty increased
        1).join("0")){
                this.nonce;
                this.hash = this.calculateHash();
        }
        }
}
newBlock.mineBlock();
```

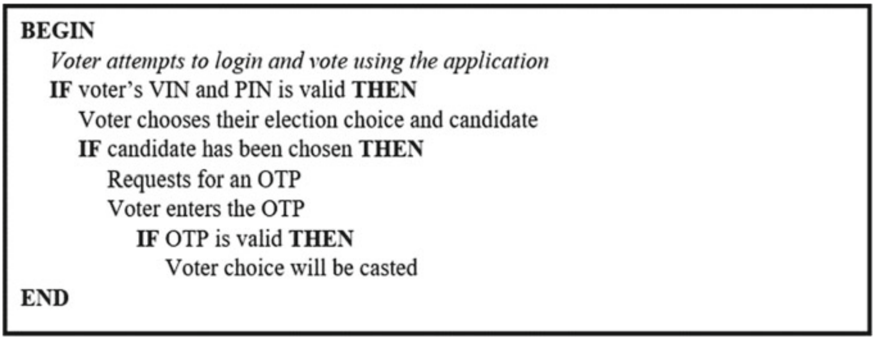
Fig. 2 Proof-of-work (PoW) algorithm

3.4 Blockchain's Proof-of-Work Algorithm

The blockchain database/ledger would require a proof-of-work (PoW) algorithm which alludes to the computational riddle/puzzle that nodes/miners need to solve that empowers the blockchain networks to stay decentralized and secured. PoW makes use of cryptographic functions that basically ensure a specific number of computer cycles which were used to solve the puzzle which proves that you did some measures of work to solve that puzzle. The amount of work is specified by the difficulty which is proportional to the amount of work needed to solve the puzzle. Miners/nodes challenge each other to identify a nonce (also called a golden nonce) that can create a hash with a value less than or equivalent to the set network difficulty. Once such a nonce is found by a miner/node, they get the privilege to add that block to the blockchain. The nonce is a focal piece of the PoW algorithm for blockchains. In this study, we would be utilizing a difficulty of four (4) and the proof-of-work is shown in Fig. 2.

3.5 Pseudocode for the Two-Factor Authentication Sequence

The two-factor authentication pseudocode sequence used in the design of the system is shown in Fig. 3. When a voter wants to make use of the application, they would have to be authenticated at both the login and voting phases. The two-factor authentication sequence shows how the authentication processes would take place at different stages.



```
BEGIN
    Voter attempts to login and vote using the application
    IF voter's VIN and PIN is valid THEN
        Voter chooses their election choice and candidate
        IF candidate has been chosen THEN
            Requests for an OTP
            Voter enters the OTP
                IF OTP is valid THEN
                    Voter choice will be casted
END
```

Fig. 3 Pseudocode of the authentication phases in the m-voting system

3.6 Voter's Activity Diagram

See Fig. 4.

3.7 Implementation Screenshots

We are making use of five modules in the implementation process. The modules are represented as follows:

1. Login and candidate selection: The system would authenticate the voter before granting them access/login them into the application using their VIN and PIN to select their preferred candidate as seen in Fig. 5.
2. Candidate selection: The system would enable the logged in voters to select their preferred candidate as seen in Fig. 6.
3. Authentication: The system would authenticate the voter before enabling them to cast their vote using OTP as seen in Fig. 7.
4. Storing of casted votes: The system would allow the storage of casted votes to the blockchain database. The hash for each vote is generated and added to the blockchain as seen in Figs. 8 and 9.
5. Results: The system would preview the results once the voting period has ended as seen in Fig. 10.

4 Results and Discussion

To test the usability of the system, ISO 9241-11 usability model with the aid of a questionnaire was utilized. Three (3) constructs were tested which are effectiveness, efficiency, and user's satisfaction. A sample of nineteen (19) citizens was asked to

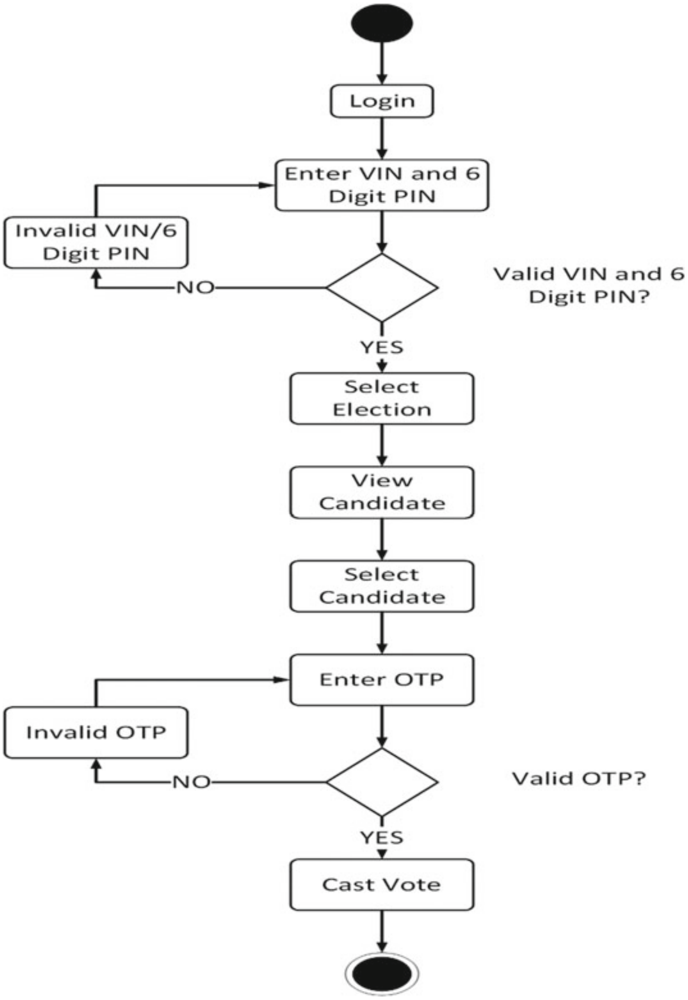


Fig. 4 An Activity Diagram showing the Activities being carried out by the Voters when utilizing the m-voting system

participate in the survey using their mobile devices. Some assumptions have to be made in order for the system to be viable, and these include the following:

1. Assumption 1: The voter's mobile device can be trusted. We accept that it is conceivable to safely run the voting application on the voter's mobile device.
2. Assumption 2: The election is correctly set up. We accept that only eligible voters can cast their votes and nothing is compromised before and during the voting procedure.
3. Assumption 3: Voters have acquired their voter's identification number (VIN) and PIN. We assume that all necessary information like age, date of birth, address, phone number, etc., have been registered at any voter's registration center in

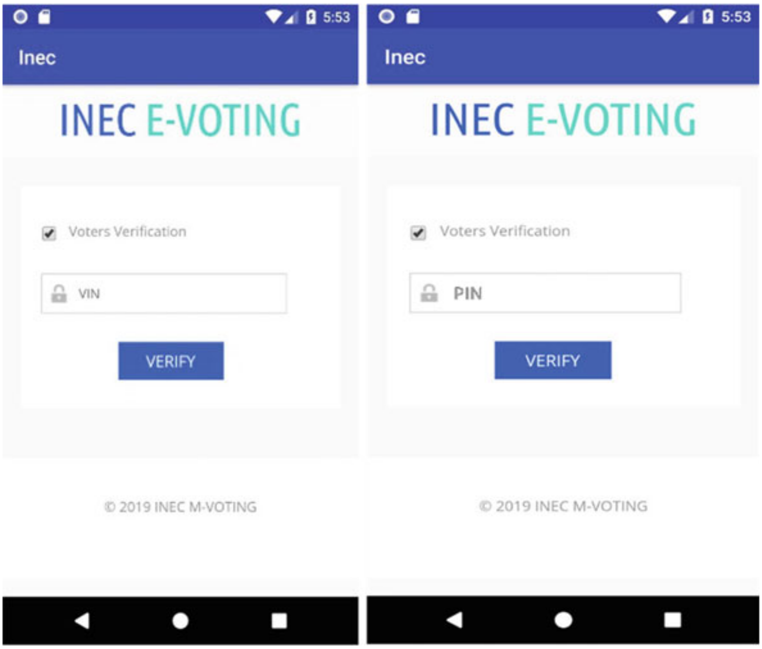
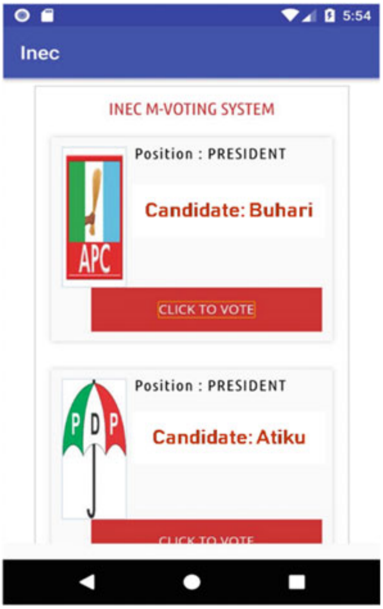
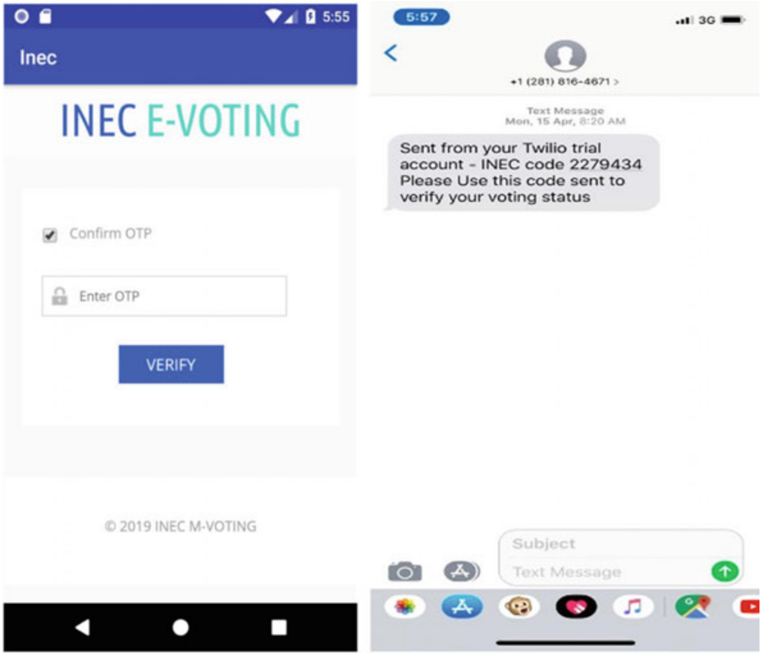


Fig. 5 Login and candidate selection interfaces

Fig. 6 Candidate selection interface



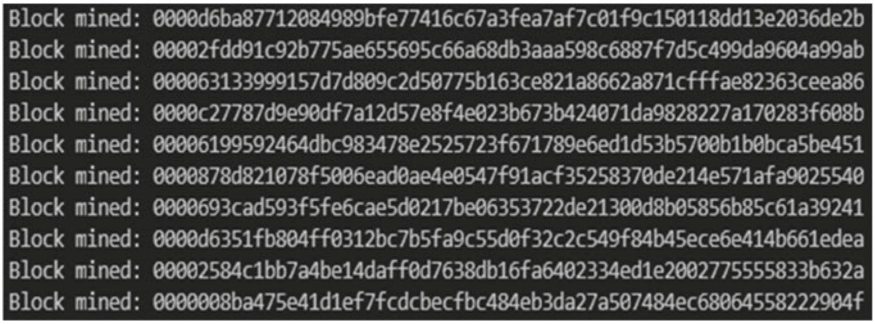


☑ Confirm OTP

Text Message
Mon, 15 Apr, 8:20 AM

Sent from your Twilio trial account - INEC code 2279434 Please Use this code sent to verify your voting status

Fig. 7 OTP authentication

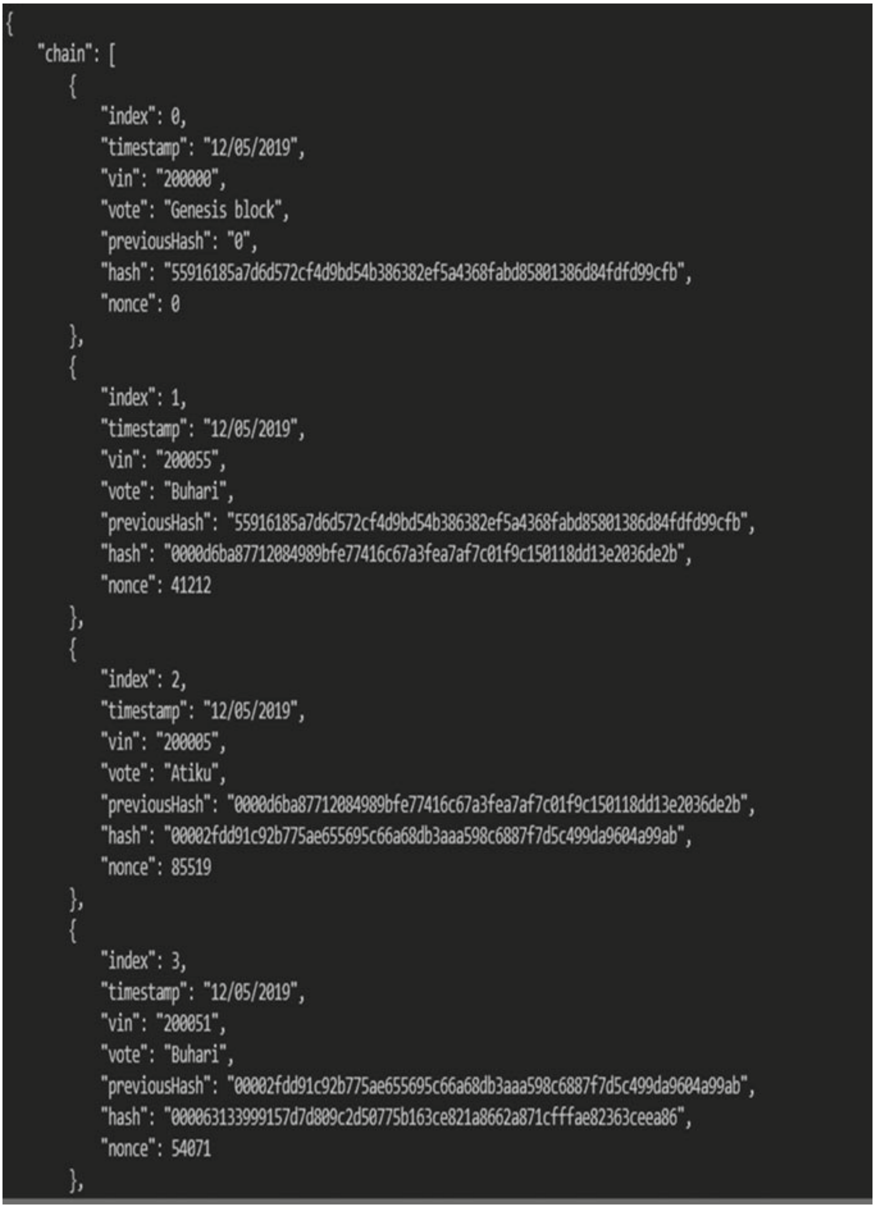


```
Block mined: 0000d6ba87712084989bfe77416c67a3fea7af7c01f9c150118dd13e2036de2b
Block mined: 00002fdd91c92b775ae655695c66a68db3aaa598c6887f7d5c499da9604a99ab
Block mined: 000063133999157d7d809c2d50775b163ce821a8662a871cfffae82363ceea86
Block mined: 0000c27787d9e90df7a12d57e8f4e023b673b424071da9828227a170283f608b
Block mined: 00006199592464dbc983478e2525723f671789e6ed1d53b5700b1b0bca5be451
Block mined: 0000878d821078f5006ead0ae4e0547f91acf35258370de214e571afa9025540
Block mined: 0000693cad593f5fe6cae5d0217be06353722de21300d8b05856b85c61a39241
Block mined: 0000d6351fb804ff0312bc7b5fa9c55d0f32c2c549f84b45ece6e414b661edea
Block mined: 00002584c1bb7a4be14daff0d7638db16fa6402334ed1e2002775555833b632a
Block mined: 0000008ba475e41d1ef7fcdcbecfbc484eb3da27a507484ec68064558222904f
```

Fig. 8 Hashes of the stored votes in the blockchain

order for them to acquire their voter's identification number (VIN) and PIN which would be utilized in the registration and voting process on the proposed system.

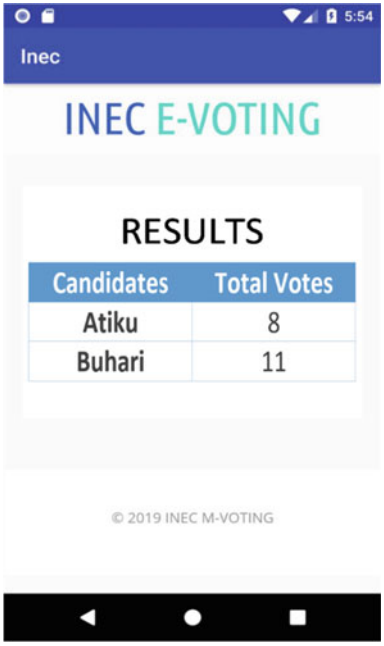
The overall score of each respondent was calculated for each usability constructed by calculating the mean based on the administered questionnaires survey scores. Strongly Agree (SA) = 5, Agree (A) = 4, Undecided (U) = 3, Disagree (D) = 2, and Strongly Disagree (SD) = 1 were utilized for the rating presented in Table 1.



```
{
   "chain": [
      {
         "index": 0,
         "timestamp": "12/05/2019",
         "vin": "200000",
         "vote": "Genesis block",
         "previousHash": "0",
         "hash": "55916185a7d6d572cf4d9bd54b386382ef5a4368fabd85801386d84fdfd99cfb",
         "nonce": 0
      },
      {
         "index": 1,
         "timestamp": "12/05/2019",
         "vin": "200055",
         "vote": "Buhari",
         "previousHash": "55916185a7d6d572cf4d9bd54b386382ef5a4368fabd85801386d84fdfd99cfb",
         "hash": "0000d6ba87712084989bfe77416c67a3fea7af7c01f9c150118dd13e2036de2b",
         "nonce": 41212
      },
      {
         "index": 2,
         "timestamp": "12/05/2019",
         "vin": "200005",
         "vote": "Atiku",
         "previousHash": "0000d6ba87712084989bfe77416c67a3fea7af7c01f9c150118dd13e2036de2b",
         "hash": "00002fdd91c92b775ae655695c66a68db3aaa598c6887f7d5c499da9604a99ab",
         "nonce": 85519
      },
      {
         "index": 3,
         "timestamp": "12/05/2019",
         "vin": "200051",
         "vote": "Buhari",
         "previousHash": "00002fdd91c92b775ae655695c66a68db3aaa598c6887f7d5c499da9604a99ab",
         "hash": "000063133999157d7d809c2d50775b163ce821a8662a871cfffae82363ceea86",
         "nonce": 54071
      },
```

Fig. 9 Contents of each block in the chain

Fig. 10 Result interface



INEC E-VOTING

RESULTS

Candidates	Total Votes
Atiku	8
Buhari	11

© 2019 INEC M-VOTING

The evaluation of the ISO 9241-11 usability model is carried out using a rating from one (1) to five (5). A system with very bad usability has 1 as its overall mean rating, bad usability has 2 as its mean rating, average usability has 3 as its mean rating, good usability has 4 as its mean rating, and excellent usability has 5 [26, 27]. From the result of the usability evaluation given in Table 1, the average effectiveness was given as 4.83, efficiency as 4.79, and user's satisfaction as 4.83. From the above analysis, it can be established that the prototype system developed has a "good usability" rating proven by the overall rating of 4.82. This system can offer multiple benefits in the electoral sector, and some of the benefits are:

- On the day of the election, eligible voters would be given access to cast their votes between a period of time and thanks to this, the government will not experience any losses since they did not declare a public holiday or the day was not called off.
- A polling station does not need to be set up due to the fact that the voters can make use of their mobile device to partake in the voting procedure which helps to reduce the high cost that is required in setting up polling stations.
- Multiple means of authentications would be utilized in order to enable the eligible voters to cast their voters and prevent illegible voters from casting theirs.
- Voters are not required to leave their homes or place of work in order to cast their votes.
- This could also provide easier accessibility of the voting procedure to multiple individuals including the elderlies and those with disabilities.
- Problems associated with the double casting of votes can be mitigated.

Table 1 Usability evaluation results collected from users

S/n	Questions	SD	D	U	A	SA	Mean
Effectiveness							
Q1	I was able to login successfully into the mobile application using my VIN and PIN	0	0	0	4	15	4.79
Q2	I was able to cast my vote successfully using the mobile application	0	0	0	5	14	4.74
Q3	I was able to use the OTP (one-time-password) to complete the voting process	0	0	0	1	18	4.95
Total							4.83
Efficiency							
Q4	I was able to use the application on my mobile device without any issue	0	0	0	7	12	4.63
Q5	I did not have to carry out too difficult steps before completing the voting process	0	0	0	2	17	4.89
Q6	The application response time was satisfactory	0	0	0	3	16	4.84
Total							4.79
User's satisfaction							
Q7	I feel comfortable using the mobile application compared to the existing voting procedure	0	0	0	0	19	5.00
Q8	There was no difficult step (s) involved in the use of the mobile application	0	0	0	1	18	4.95
Q9	I would use the application for casting my vote over the existing method	0	0	0	9	10	4.53
Total							4.83
Total mean							4.82

- The casting of votes and tallying of the votes would be a lot quicker while also providing better transparency and accuracy.
- The casted votes would be safely and securely stored in the blockchain database which would mitigate any form of manipulation or tampering like the deletion of legitimate votes or the addition of illegitimate votes.
- There will be a progressive increment in the number of youths taking part in the voting procedure.

With this voting system, a level of resiliency can be attained and is presented in the graph as shown in Fig. 11. This is measured on a scale of 1–5. 1 meaning "Worst", 2 meaning "Bad", 3 meaning "Average", 4 meaning "Good", and 5 meaning "Very Good".

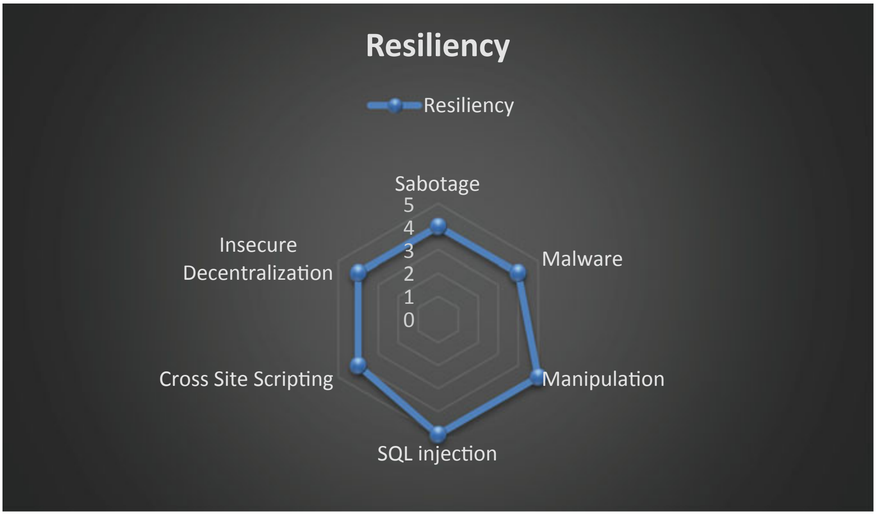


Fig. 11 Resiliency graph of the m-voting system

5 Conclusion

In this article, VIN, PIN, and OTP were utilized as the credentials needed for the authentication process. Blockchain technology was also utilized as a database to securely store the cast votes and mitigate any form of tampering in the process. The result of this study has shown a good usability rating which implies that the system is viable and can be implemented to solve the identified problems. This system is expected to securely protect the casted votes and verify voter's eligibility to cast their votes while providing an easily accessible voting system. This study has contributed to the body of knowledge by developing a mobile voting system that integrates blockchain technology and two-factor authentication to provide a secure and easy means of election participation which enables citizens to cast their votes using their mobile devices, storing, and securing the casted votes while offering better transparency. For future works, the system can be made to support multiple language types so as to better improve the usability rating and provide a better multilingual system to different language speaking types.

Acknowledgements We would like to acknowledge the sponsorship and support provided by Covenant University through the Centre for Research, Innovation, and Discovery (CUCRID).

References

1. Shuaibu, A., Mohammed, A., Ume, A.: A framework for the adoption of electronic voting system in Nigeria. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **7**(3), 258–268 (2017)
2. Folarin, S., Ayo, C., Oni, A., Gberevbie, D.: Challenges and prospects of e-Elections in Nigeria. In: European Conference on e-Government, pp. 93–100. ACPI, England (2014)
3. Ayo, C.K., Ekong, U.O., Ikhu-omoregbe, N.A., Ekong, V.E.: M-voting implementation: the issues and trends. http://www.academia.edu/download/3258019/EEE4041.pdf. Last accessed 22 Sept 2019
4. Ananti, M.O., Onyekwelu, R.U.: Election and conundrum of sustainability of democracy in Nigeria. J. Policy Develop. Stud. **11**(5), 57–62 (2018)
5. Shaibu, M.E.: Nigerian election management bodies and their associated election challenges. Asian Int. J. Soc. Sci. **18**(1), 21–42 (2018)
6. Inuwa, I., Oye, N.D.: The impact of e-voting in developing countries: focus on nigeria. Am. J. Eng. Res. (AJER) **30**(2), 43–53 (2015)
7. Ekong, U., Ayo, C.: The prospects of m-voting implementation in Nigeria. In: Proceedings of the International Conference & Workshop on 3rd Generation (3G) GSM & Mobile Computing: An Emerging Growth Engine for National Development, pp. 172–179. Covenant University, Nigeria (2007)
8. Kayode, A.A., Olalekan, I.A.: A biometric e-voting framework for Nigeria. Jurnal Teknologi **77**(13), 37–40 (2015)
9. Vince, T.: Databases and Blockchains, the Difference is in Their Purpose and Design. https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b. Last accessed 22 Sept 2019
10. Thomas, M.: Security and privacy via optimised blockchain. Int. J. Adv. Trends Comput. Sci. Eng. **8**(3), 415–418 (2019)
11. Curran, K.: E-voting on the blockchain. J. British Blockchain Assoc. **1**(2), 1–6 (2018)
12. Bailon, M.R.M.: International roaming services optimization using private blockchain and smart contracts. Int. J. Adv. Trends Comput. Sci. Eng. **8**(3), 544–550 (2019)
13. Fusco, F., Lunesu, M.I., Pani, F.E., Pinna, A.: Crypto-voting, a blockchain based e-voting system. In: 10th International Proceedings of the Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 223–227. SCITEPRESS, Spain (2018)
14. Shaan, R.: The Difference Between Blockchains & Distributed Ledger Technology. https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92. Last accessed 20 Sept 2019
15. Uzedhe, G., Okhaifoh, J.E.: A technological framework for transparent e-voting solution in the Nigerian electoral system. Nigerian J. Technol. (NIJOTECH) **35**(3), 627–636 (2016)
16. Mpekoa, N., Greunen, D.: m-voting: understanding the complexities of its implementation. Int. J. Digital Soc. **7**(4), 1214–1221 (2016)
17. Nwabueze, E.E., Obioha, I., Onuoha, O.: Enhancing multi-factor authentication in modern computing. Sci. Res. Publish. Commun. Netw. **9**(3), 172–178 (2017)
18. Alausa, D.W.S., Ogunyinka, O.I.: The effect of e-voting and the alternative ballot box In Nigeria. Am. J. Eng. Res. (AJER) **6**(8), 46–55 (2017)
19. Yavuz, E., Koc, A.K., Cabuk, U.C., Dalkilic, G.: Towards secure e-voting using ethereum blockchain. In: 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–7. IEEE, Turkey (2018)
20. Wu, H.-T., Yang, C.-Y.: A blockchain-based network security mechanism for voting systems. In: 1st International Cognitive Cities Conference (IC3), pp. 227–230. IEEE, Japan (2018)
21. Sakinah, B.N., Hafizhelmi, K.Z.F., Ihsan, M.Y.A., Nooritawati, M.T.: Blockchain in voting system application. Int. J. Eng. Technol. **7**(4.11), 156–162 (2018)
22. Purandare, H.V., Saini, A.R., Pereira, F.D., Mathew, B., Patil, P.S.: Application for online voting system using android device. In: International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–5. IEEE, India (2018)

23. Kshetri, N., Voas, J.: Blockchain-enabled e-voting. IEEE Softw. **35**(4), 95–99 (2018)
24. Gajabe, J.: Implementation of mobility based secured e-voting system. Int. J. Res. Appl. Sci. Eng. Technol. **6**(3), 3449–3454 (2018)
25. Gentles, D., Sankaranarayanan, S.: Biometric secured mobile voting. In: 2nd Asian Himalayas International Conference on Internet (AH-ICI), pp. 1–6. IEEE, New Jersey (2011)
26. Sauro, J., Kindlund, E.: A method to standardize usability metrics into a single score. In: Proceedings of the SIGCHI Conference on Human factors in Computing Systems—CHI 2005, pp. 401–409. ACM Press, New York (2005)
27. Nielsen, J., Levy, J.: Measuring usability: preference versus performance. Commun. ACM **37**(4), 66–75 (1994)