Quest Journals
Journal of Software Engineering and Simulation
Volume 8 ~ Issue 6 (2022) pp: 48-52
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

E-Voting Framework Utilizing Blockchain Technology & Multi Factor Authentication

1. Guide Prof. Shaheen Mujawar, 2. Ms. Sakshi B, 3. Ms. Keerti, 4. Ms. Jytoti , 5. Ms. Ruhama

Department of Computer Science and Engineering, S. G. Balekundri Institute of Technology, Belagavi, KA, India – 590010

Abstract:
E-VOTING IS AMONG the key public sectors that can be disrupted by blockchain technology.1 The idea in blockchain- enabled e-voting (BEV) is simple. To use a digital- currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline.2 Here, we argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud. The idea is as follows. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamperproof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record. No bad actor can engage in nefarious activities because such activities will be evident on the ledger or corrected by a peer-to-peer consensus network.3 To compromise the network, hackers would need to successfully hack most of the blocks (files with transaction records) before new blocks were introduced. 3 The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added.4 Put simply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approach's potential benefits and challenges.

Keywords—Blockchain , AES, DES, Hash Algorithm Django;

*Received 15 June, 2022; Revised 28 June, 2022; Accepted 30 June, 2022 © The author(s) 2022. Published with open access at **www.questjournals.org***

I. INTRODUCTION

The use of mobile phones be utilized by the citizens to efficiently, securely and easily partake in the voting process. They noted that mobile devices being utilized in the voting process cannot only save time but cost as well and could be used as a secure method for casting their ballots or votes. a mobile voting application was designed that enables voter's to easily cast their vote using their mobile devices. The voter would download the application and cast their votes which would be stored on a centralized database. This meant that the votes were being managed by an administrator and the stored votes could be changed by a malicious insider or the admin. Since it is a centralized database, it is susceptible to DDoS attacks. also noted the same problem in their proposed mobile voting system which also made use of a centralized database to store the vote. stated that blockchain serves as a public ledger of transactions which cannot be reversed and can be used to store the casted votes but the cost in setting up powerful nodes for the distributed blockchain system was too high. A novel electronic voting system based on blockchain was proposed by that aimed to improves security while also reducing the expense of carrying out an election. Their proposed system would require a powerful dedicated system situated at each polling unit meaning that voters still have to queue to cast their votes and the cost of implementing this would be high.

An Auditable Blockchain Voting System (ABVS) was designed by [9] which would enable easy audit and verification of the voting process using distributed blockchain technology. They also noted that powerful systems would have to be implemented at the voting polls which meant that citizens would still need to leave their homes or places of residence to cast their votes while also consume a lot of electrical energy increasing the setup cost compared to a paper-based voting system.

II. EXISTING SYSYTEM

In order to make the voting process more effective the institutions like 'Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free, and fair elections. The concept of secret voting was introduced since the beginning of the voting system. Since the trust on democratic systems is increasing it is important to uphold that the trust on voting should not decrease. In the recent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments.Since all these countries are among the emerging democracies, it is pretty likely that in next decades they will emerge as full democracies and the vote and the voting process willearn more respect and trust over time.

III. PROPOSED SYSTEM

The voters name must exist in the voting list to enable himself to visit the polling station for the purpose of voting. It is the responsibility of the voter himself to ensure that once he attained the age of eighteen years, his name should be present in the voting list. This can be done by consulting the respective offices, e.g. National Database and Registration Authority (NADRA) in Pakistan. The voting lists are published few weeks earlier than the elections. The individual having his name in the voting list is eligible to vote and presents his original identity to the polling staff. Before casting the vote, the voter has to be authenticated by the biometric system. The record of the voter is checked with the help of NADRA's database.Once the voter has passed the authentications check, he is brought to voting screen to vote. From the voting machine the names and respective party symbols of each candidate are displayed and the voter can vote according to his will. The confirmation screen seeks the confirmation of the voter and records the vote casted by the voter.The voter can vote only once, and once the vote is casted is voting record is marked as ''voted'', which restricts the voters from voting again. The name of the voter can be blocked or eliminated from the list of eligible voters list for the current elections, once he has casted the vote.The polling process continues until the voting time ends or all the voters in the voting list have casted their votes.

A. Problem Definition

Voting is fundamental to any consensus-based society and is one of the most critical functions of democracy. Mobile voting (m-voting) was utilized as a means for voters to easily and conveniently cast their votes using their mobile devices which have been the most adopted means of communication but has a major problem which is safely securing the casted votes and avoiding any form of tampering.

IV. LITERATURE SURVEY

[19] proposed the use of mobile phones be utilized by the citizens to efficiently, securely and easily partake in the voting process. They noted that mobile devices being utilized in the voting process cannot only save time but cost as well and could be used as a secure method for casting their ballots or votes. In a study by [20], a mobile voting application was designed that enables voter's to easily cast their vote using their mobile devices. The voter would download the application and cast their votes which would be stored on a centralized database. This meant that the votes were being managed by an administrator and the stored votes could be changed by a malicious insider or the admin. Since it is a centralized database, it is susceptible to DDoS attacks. [21] also noted the same problem in their proposed mobile voting system which also made use of a centralized database to store the vote. [9] stated that blockchain serves as a public ledger of transactions which cannot be reversed and can be used to store the casted votes but the cost in setting up powerful nodes for the distributed blockchain system was too high. A novel electronic voting system based on blockchain was proposed by [9] that aimed to improves security while also reducing the expense of carrying out an election. Their proposed system would require a powerful dedicated system situated at each polling unit meaning that voters still have to queue to cast their votes and the cost of implementing this would be high.

An Auditable Blockchain Voting System (ABVS) was designed by [9] which would enable easy audit and verification of the voting process using distributed blockchain technology. They also noted that powerful systems would have to be implemented at the voting polls which meant that citizens would still need to leave their homes or places of residence to cast their votes while also consume a lot of electrical energy increasing the setup cost compared to a paper-based voting system. [22] noted that voting is significant and it's still being engaged in by physically going to voting booths which is susceptible to tampering and does not guarantee security. They developed an online voting application using Ethereum blockchain to combat these issues, however, a voter would need a pretty powerful system to partake in the voting process and sometime their system could be utilized as a node to aid in the mining process. Each of the research work introduced different

means to provide an easily accessible and secured m-voting system with or without the utilization of blockchain technology..

V. METHODOLOGY

A. Polling Process

The electronic voting system is executed in a way that it deploys many individuals at different levels. In order to develop an effective block creation system, it is important to understand the actual execution on ground. In the conduct of the elections, the election commission and the NADRA (National Database and Registration Authority) have a big role to play. NADRA is the national registration authority in Pakistan and is responsible for the registration and issuance of identity documents to the citizens of Pakistan. The NADRA is responsible to ensure that each citizen of the country has its record available and the biometrics of each individual are also available . The biometric authentication is used in the voter's authentication on the polling day. The election commission is responsible for making the electoral lists available which are verifiable from the base records. The authenticated voters can vote according to the provision provided to them and the usage of technology is made toget the vote recorded and tabulated accordingly. It is also the responsibility of the election commission to declare the results when polling station wise and constituency wise tabulation has been made.

B. Blockchain

Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain.Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will . This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively . This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

C. Hashing

Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different level.MD5 algorithm is widely used for hashing purposes and it provides a 128 nit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed [40]. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerabilities. Race Integrity Primitive Evaluation Message Digest(RIPEMD) is a family of hash function developed by Hans Dobbertin in 1996. This algorithm was designed to replace the MD5 as a more secure alternative. It has few variations that have emerged over time including RIPEMD-128, RIPEMD-160, RIPEMD256, and RIPEMD-320.

D. Proofs

In Proof of work deals with the mining / creation of the blocks in such a way that it can be proved that a significant effort has been made for the resolution of the mathematical problem introduced for the creation of a block in the blockchain. The mathematical complexity is increased on the creation of every new block so make the creation of the block complex and a rewarding scenario. The increasing complexity is introduced with the help of the hash functions, marckle trees, and the nonce value. In Proof of Stakerevolves around the identification of the stakes in the blockchain. The holders of assets are subject to have more priority in the creation of the blocks. The likelihood of that only few creators of the blocks may control the entire blockchain by virtue of the assets that they have, can't be ignored. This concept is applicable in the consortium blockchain or the private blockchain where the holding companies may need an administrative access to the blockchain.Proof of Burnn deals with the burning of the coins that are gained over a period of time . This burning process works as a fuel for the creation of new blocks. This proof of burn concept ensures that the individuals don't become powerful enough by increasing their stakes in the network. The burn process is recorded by sending the coins / proof of work to an arbitrary address, that may be designated by the network itself.

Modules to be used- The proposed framework is divided into two layers which are the front end and back end that was also adapted.

1. **Front End Layer:** This layer is categorized into two phases which are the preelection phase (can be utilized by the voters to register themselves and is stored in the voter's database) and the election phase (voters using their mobile devices can cast their votes).

2. **Back End Layer:** This layer deals with the blockchain database that can be viewed and monitored by the EMBs which is carried out at the post-election phase. Here, the casted votes are stored in the blockchain distributed database and once the election phase is over, the votes would be tallied and the final result would also be presented or shown.

Laptop: Used to run our code. 4.4 Webcam: Used to get the video feed.

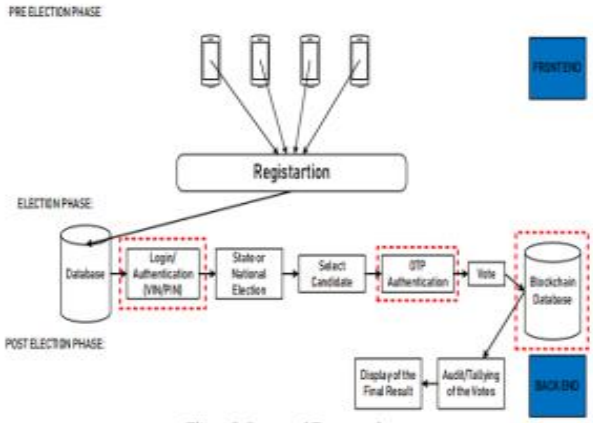

Fig. 2: Data Flow Diagram

E. OBJECTIVES

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user -friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant.

VI. FUTURE SCOPE

We have demonstrated that blockchain can significantly simplify the task of electronic voting meanwhile ensures many desired security prop erties. Recent research also shows that voting may violate Arrow's impossibility theorem in classical voting, which in a sense demonstrates that quantum information is valuable for democracy. In the future, we will further improve our protocol such that it has various advantages in both security and democracy.

VII. CONCLUSION

Mistrust in the voting is not an uncommon phenomenon even in the developed countries. The electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. The electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep consideration by the legislatures, technologist, civil society, andthe people. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

REFERENCES

[1]. Olusola, O., & Adesina, R. (2015). A Framework for Electronic Voting in Nigeria. International Journal of Computer Applications, 129(3), 12–16. https://doi.org/10.5120/ijca2015906786

[2]. Shuaibu, A., Mohammed, A., & Ume, A. (2017). A Framework for the Adoption of Electronic Voting System in Nigeria. International Journal of Advanced Research in Computer Science and Software Engineering, 7(3), 258–268. https://doi.org/10.23956/ijarcsse/V7I3/01310

[3]. Qadah, G. Z., & Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. Computer Standards & Interfaces, 29(3), 376–386. https://doi.org/10.1016/j.csi.2006.06.001

[4]. Khelifi, A., Grisi, Y., Soufi, D., Mohanad, D., & Shastry, P. V. S. (2013). M-Vote: A Reliable and Highly Secure Mobile Voting System. 2013 Palestinian International Conference on Information and Communication Technology, 90–98. https://doi.org/10.1109/PICICT.2013.25

[5]. Ayo, C. K., Ekong, U. O., Ikhu-omoregbe, N. A., & Ekong, V. E. (2007). M-voting implementation: The issues and trends. 1–5. Retrieved from http://www.academia.edu/download/3258019/EEE4041.pdf

[6]. [6] Ekong, O. U., & Ekong, E. V. (2010). M-Voting: A Panacea for Enhanced E Participation. Asian Journal of Information Technology, 9(2), 111–116. https://doi.org/10.3923/ajit.2010.111.116

[7]. Inuwa, I., & Oye, N. D. (2015). The Impact of E-Voting in Developing Countries: Focus on Nigeria. International Journal of Pure and Applied Sciences and Technology, 30(2), 43–53. Retrieved from https://search.proquest.com/docview/1762442479?accountid=8144%0Ahttp://sfx.aub .aau.dk/sfxaub?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%3 Ascitechpremium&atitle=The+Impact+of+E-Voting+in+Developing+Countries%3A

[8]. Kayode, A. A., & Olalekan, I. A. (2015). A BIOMETRIC E-VOTING FRAMEWORK FOR NIGERIA. Jurnal Teknologi, 77(13), 37–40. https://doi.org/10.11113/jt.v77.6363

[9]. Curran, K. (2018). E-Voting on the Blockchain. The Journal of the British Blockchain Association, 1(2), 1–6. https://doi.org/10.31585/jbba-1-2-(3)2018

[10]. Shaan, R. (2018). The Difference Between Blockchains & Distributed Ledger Technology. Retrieved March 22, 2019, from Towards Data Science website: https://towardsdatascience.com/the-difference-between-blockchains-distributed ledger-technology-42715a0fa92

[11]. Uzedhe, G., & Okhaifoh, J. E. (2016). A TECHNOLOGICAL FRAMEWORK FOR TRANSPARENT E-VOTING SOLUTION IN THE NIGERIAN ELECTORAL SYSTEM. Nigerian Journal of Technology (NIJOTECH), 35(3), 627–636. https://doi.org/sci-hub.tw/10.4314/njt.v35i3.22

[12]. Mpekoa, N., & Greunen, D. (2016). m-Voting: Understanding the complexities of its implementation. International Journal for Digital Society, 7(4), 1214–1221. https://doi.org/10.20533/ijds.2040.2570.2016.0149

[13]. Nwabueze, E. E., Obioha, I., & Onuoha, O. (2017). Enhancing Multi-Factor Authentication in Modern Computing. Communications and Network, 09(03), 172– 178. https://doi.org/10.4236/cn.2017.93012

[14]. Odun-Ayo, I., Odede, B., & Ahuja, R. (2018). Cloud Applications Management – Issues and Developments. In O. Gervasi, B. Murgante, S. Misra, E. Stankova, C. M. Torre, A. M. A. C. Rocha, … Y. Ryu (Eds.), Computational Science and Its Applications – ICCSA 2018 (Vol. 10964, pp. 683–694). https://doi.org/10.1007/978- 3-319-95171-3_54

[15]. Jake, F. (2018). Blockchain-as-a-Service (BaaS). Retrieved February 13, 2019, from https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp

[16]. Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 983–986. https://doi.org/10.1109/CLOUD.2018.00151

[17]. Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a Blockchain based e-Voting System. Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, 3, 223– 227. https://doi.org/10.5220/0006962102230227

[18]. Aran, D. (n.d.). How to Use Blockchain to Build a Scalable Database? Retrieved February 12, 2019, from https://www.devteam.space/blog/how-to-use-blockchain-to build-a-scalable-database/

[19]. Kogeda, O. P., & Mpekoa, N. (2010). Model for A Mobile Phone Voting System for South Africa. Journal of Computer Science and Mobile Technology, 12(3), 1–15. Retrieved from http://www.researchgate.net/profile/Okuthe_Kogeda/publication/256815434_Model_ for_A_Mobile_Phone_Voting_System_for_South_Africa/links/00463523c9c776f48d 000000.pdf

[20]. Mpekoa, N. (2014). Designing, developing and testing a mobile phone voting system in the South African context. In J. Steyn & D. Van Greunen (Eds.), Proceedings of the 8th International Development Informatics Association Conference (pp. 372–385). https://doi.org/10.1016/J.GEODERMA.2014.11.014 [21] Hegde, A., Anand, C., & Jyothi, B. (2017). Mobile Voting System. International Journal of Science, Engineering and Technology Research (IJSETR), 6(4), 2–6. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&cad=rja