WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Electronic Voting System Based on Blockchain Technology

K Swaroopa[1], E Sanghavi[2], G Murali[3] and M Eranna[4]

[1,2,3,4]Aditya Engineering College, Surampalem, AP, India.

ABSTRACT:

Democracy elections are important and grave incident anywhere. the present electoral system anywhere—in a school, institution, or even a country—uses paper ballots or electronic voting machines. There are many drawbacks to this process, including lack of transparency, low voter participation, vote tampering, distrust of electoral officials, delays in results, and, most importantly, security concerns. Therefore, the development of digital technology today has improved the livelihoods of many. To counteract the drawbacks of the current voting method, electronic voting is proposed. In essence, electronic voting is a way to submit and tally ballots electronically. It is a quick, inexpensive, and secure method to carry out a voting process that requires high security and is data-rich and real-time. Concerns about the privacy of messages and network security for electronic voting have grown recently. As a result, the availability of computerized voting is urgently needed and is growing in popularity in networking and communication. Blockchain technology is one method to address security issues. In order to develop an electronic polling system using a blockchain, the paper suggests a new system that tackles some of the drawbacks in current systems and assesses some of the well-known blockchain frameworks. The implementation outcome demonstrates that using the blockchain, you can create an efficient and secure electronic voting method. It resolves the issue of vote fraud in computerized elections because the blockchain stores its data in a decentralized way. Direct network apps can use the electronic voting system built on a blockchain.

Introduction

Overview:

This project's primary idea is to conduct voting in a secure manner while allowing people to cast their ballots online. It employs face recognition technology to authenticate the user, solving the issue of dummy entries. As a result, this method ensures that there can be no election fraud and that voting will be simple, requiring voters to stay inside to cast their ballots.

Objective

The primary goal of electronic voting technology is to speed up ballot counting, lower the cost of paying staff to physically count ballots, and improve accessibility for voters with disabilities.

This can be accomplished by planning and creating a software framework for voter registration, election voting, real-time election results collation and monitoring, and primarily for remote voter access to elections.

Research and put into practice a security method that will be used to guarantee that votes submitted in the system won't be compromised and that no external attack would be encountered, which will be guaranteed by blockchain technology.

Proposed System:

- This approach involves these steps.
- Based on our current system implementation, we now explain an average user engagement with the suggested scheme. In essence, the voter logs into the system by having their visage scanned. The facial recognition system verifies the voter after scanning their visage. If a match is discovered, the voter is shown a selection of potential candidates and given the chance to reject them. If the match is unsuccessful, entry would instead be restricted. This functionality is made possible by implementing an authentication method (in this instance, a facial recognition system) properly and using predefined role-based access control.
- Votes that have been properly cast are added to the public ledger after being verified by a number of miners. Voting security is built on blockchain technology, which secures end-to-end verification using cryptographic hashes. A valid vote is treated as a blockchain transaction for this reason. As a result, the casting vote is added to the blockchain as a new block (after successful mining) and is also noted in the data files at the database's end.

- The system guarantees that each voting system belongs to a single person with a single vote. In order to avoid double voting.
- Following the validation procedure, the voter is instantly notified via text message or email with the transaction ID mentioned above, allowing them to follow their vote to the ledger. While serving as a voter notification, this protects voters' privacy by not allowing anyone to find out how a specific voter chose. It's essential to note that the voter's cryptographic hash is the only hash by which the voter can be identified in the blockchain.
- The complete voting process can be more easily verified thanks to this feature. Furthermore, this ID is concealed and inaccessible; This hash cannot even be seen by the system operator or supervisor, ensuring the anonymity of each voter.

Advantages:

- Enhanced security due to the use of secure communication routes for voting.
- Minimal setup costs because only the cost of an internet connection is necessary to cast a ballot on all of the available e-voting platforms.
- Speedy vote counting and accurate findings.
- Reduced human involvement leads to fraud prevention.

Architecture:

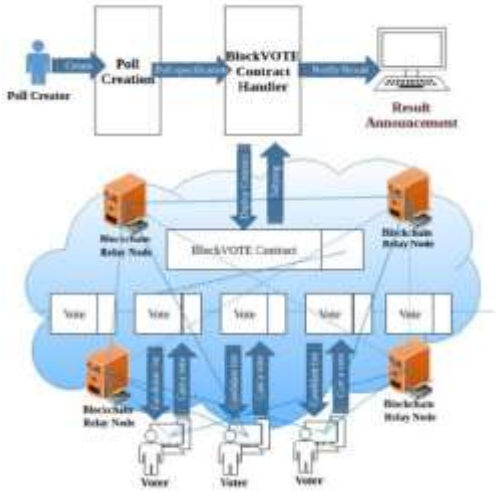


Fig.1 Architecture Diagram

Hardware Requirements:

- **Processor type:** Intel core i5 and above
- **Processor speed:** Minimum 2.00 GHz and above
- **RAM:** 6-10 GB
- **Hard disk:** 400 GB or more
- **Monitor:** 800x600 or higher resolution
- **Keyboard:** 110 keys enhanced

Software Requirements:

- **Front-End:** React-js
- **Back-end:** Solidity
- **IDE:** VS Code

Modules:

- Login

- Voting
- Voting Creation

- Voting Result
- User Identification

Login:

There are two different kinds of logins, which are discussed in this module's section on login functionality. Admin Login is followed by User Login.

Voting:

Voting is available in this section for users. This lesson will outline a complete page that lists all of the candidates and indicates them with symbols.

Voting Creation:

The entire voting setting can be created in admin (i.e. arrange voting facility, specifies time of voting, add candidates that have stand, and records the entry that particular person has voted, etc.)

Voting Result:

As it provides the polling results, this module serves as our system's primary module. Our votes won't be tampered with because we used blockchain technology, ensuring that the right contender will win and maintaining their integrity.

User Identification:

This module system will verify whether a specific person is legitimate or not. In order to make the voting process clear and ensure that no one can submit a vote on someone else's behalf, this authentication will be carried out by a face recognition system, which requires users to scan their faces in order to access the voting portal.

Data Flow Diagram:

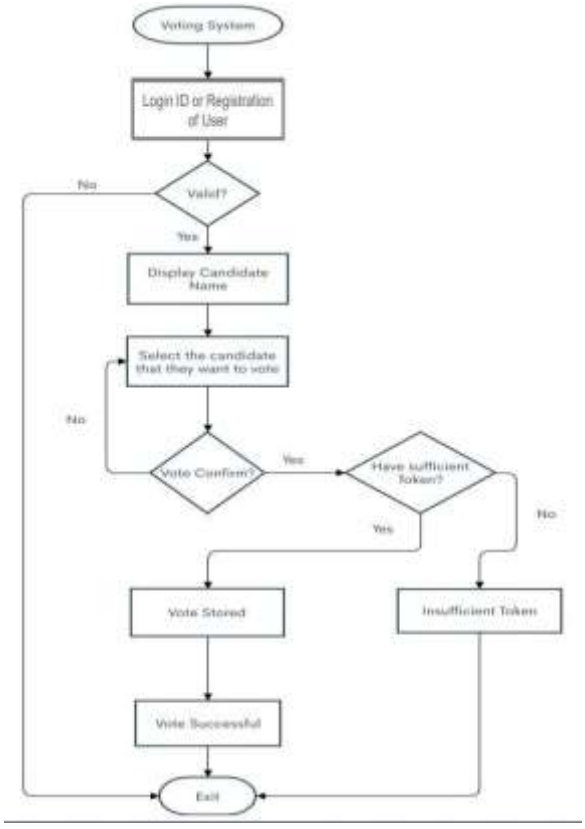
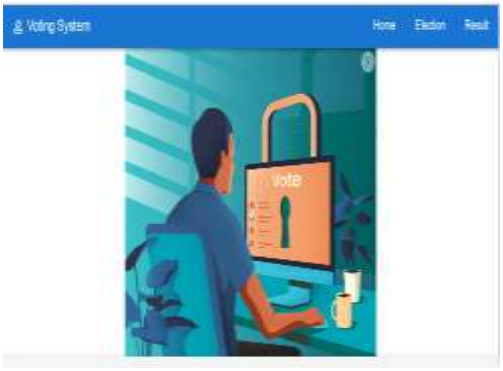


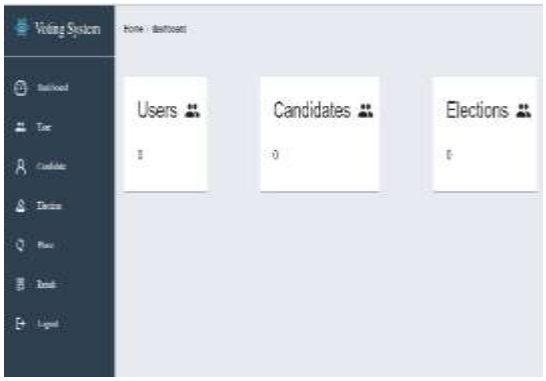
Fig.2 Data Flow Diagram

Result:

Home page



Admin Dashboard



View users

Candidates

Conclusion:

In any democratic community, a trustworthy and honest voting process is essential. Elections must be reliable for democracies to function effectively, and voters must have faith in the process. Elections conducted on paper in the past, however, lack credibility. Modern society finds the concept of modifying digital voting systems to simplify, speed up, and reduce the cost of public elections appealing.

Making the voting process simple and fast normalizes it in the eyes of the electorate, lowers the power gap between them and the elected officials, and puts some pressure on them. Additionally, it creates a space for a director form of democracy where citizens can voice their opinions on particular proposals and legislation.

Smart contracts have been used in this project to create a voter privacy is guaranteed by a blockchain-based voting method. while enabling safe and affordable elections. In addition to a security study of the system, it describes the system's architecture and design.

References:

1. R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting", *Symmetry*, vol. 12, no. 8, pp. 1328, Aug. 2020.
2. 5. Onuklu, A. (2019), "Research on Blockchain: A Descriptive Survey of the Literature", Choi, J. and Ozkan, B. (Ed.) Disruptive Innovation in Business and Finance in the Digital World (International Finance Review, Vol. 20), Emerald Publishing Limited, pp. 131-148. DOI/10.1108/S1569-3767201
3. Zhang K, Zhang Z, Li Z, et al. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks [J]. IEEE Signal Processing Letters, 2016, 23(10):1499-1503.
4. Pranav KB, Manikandan J, " Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks", April 2020, ScienceDirect
5. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* 2019, *7*, 24477–24488.
6. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* 2019, *7*, 115304–115316.
7. Ramya Govindaraj, P Kumaresan, K. Sree harshitha, " Online Voting System using Cloud," 24-25 Feb. 2020, IEEE
8. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* 2020, *8*, 21091–21116.
9. Yi, H. Securing e-voting based on blockchain in P2P network. *EURASIP J. Wirel. Commun. Netw.* 2019, *2019*, 137.
10. Torra, V. Random dictatorship for privacy-preserving social choice. *Int. J. Inf. Secur.* 2019, *19*, 537–543.
11. Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. *Comput. Sci. Rev.* 2020, *36*, 100235.
12. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput.Syst.* 2020, *105*, 13–26.