iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59416

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

A Voting System Based on Blockchain Technology

M. Srikanth[1], G. Supriya[2], Ms. N. Surekha[3]
[1, 2]*B.Tech, Computer Science and Engineering*
[3]*Assistant Professor, Department of Computer Science and Engineering*

Abstract: ***Electronic voting, also known as e-voting, has been utilized in various forms since the 1970s. It offers significant advantages over traditional paper-based systems, such as improved efficiency and reduced errors. However, there are still obstacles to overcome in order to widely adopt e-voting systems, particularly in terms of enhancing their resilience against potential faults. Blockchain, a revolutionary technology of our time, holds the potential to enhance the overall resilience of e-voting systems. This research paper aims to leverage the benefits of block-chain, including cryptographic foundations and transparency, to develop an effective e-voting scheme. The proposed scheme adheres to the fundamental requirements for e-voting systems and achieves end-to-end verifiability. The paper provides a comprehensive overview of the proposed e-voting scheme and its implementation using the Multichain platform. Furthermore, it presents a thorough evaluation of the scheme, successfully demonstrating its effectiveness in achieving an end-to-end verifiable e-voting system***
Keywords: Electronic voting, e-voting, blockchain, e-government, verifiable voting.

I. INTRODUCTION

Blockchain technology is really changing up how we vote these days, which is pretty cool. It lets every vote get locked in encrypted and put on this long chain of blocks where no one can secretly change anything after people vote and since we don't need any third parties to get involved, it's a lot harder for shady stuff to happen behind the scenes too. Voters can just check on their vote whenever they want, which makes the whole system more see-through. That's a big upgrade for trust! When you add up all of blockchains advantages for safety and access it really might lead to better elections that work for everybody. Democracy wins all around.

Blockchain tech has possible uses beyond finance, like changing up traditional ways companies do business. It could remove middlemen, cutting costs and speeding things up since it's decentralized and smart contracts that carry out agreements automatically could also improve stuff across industries.

Plus, blockchain may fix hacking fraud, estc by storing data securely. It's tamper-proof and decentralized so it makes sure info checks out. This matters for sectors needing trust and security.

As blockchain evolves and spreads, it could impact the economy and society big time. With the potential to shake up industries, boost efficiency and enhance safety, blockchain seems ready to change how we do business and connect in the digital world.

II. RELATED WORK

A. Literature Review

Adida, B., Helios (2008) presented a research paper titled "Web-based open-audit voting" at the 17th Conference on Security Symposium, ser. SS'08. The paper suggests a suitable security model and criteria to assess comprehensibility. Furthermore, it introduces a web ballot system called "Pretty graspable Democracy" and demonstrates that it meets the requirements of the proposed security model. Interestingly, it is found to be more user-friendly compared to the existing system, "Pretty smart Democracy," which also fulfills the proposed security model.

The article by Chaum et al. (2008) introduces Scantegrity, a groundbreaking End-to-End (E2E) verification system designed specifically for optical-scan voting. This innovative system aims to ensure the integrity of elections while also allowing for manual recounts, without causing any disruptions. Traditional optical-scan voting systems have been widely used due to their efficiency and accuracy. However, concerns have been raised regarding the potential for tampering or manipulation of the voting process. This is particularly worrisome as manual recounts, which are crucial for verifying the accuracy of the results, can be time-consuming and prone to errors. Scantegrity addresses these concerns by introducing a unique approach to E2E verification. The system combines cryptographic techniques with optical-scan technology to create a secure and transparent voting process. It allows voters to verify that their votes have been accurately recorded and counted, while also ensuring that their choices remain anonymous.

During the 2012 International Conference on E-voting, Dalia, K., Ben, R., Peter Y. A, and Feng, H. presented their research paper titled "Enhancing fairness and reliability in voting systems through broadcast." The objective of their study was to propose innovative measures to improve the fairness and reliability of voting systems by incorporating certain mechanisms. One of the key contributions of their research was the introduction of a recovery round in the voting process. This recovery round aimed to address the issue of voter abandonment, which can occur when voters leave the voting process before completing it. The researchers suggested that in such cases, a recovery round should be conducted to determine the election outcome. This additional round would ensure that the election results are still valid and representative, even in the absence of some voters.

In the 2013 paper titled "Star-vote: A secure, transparent, auditable, and reliable voting system," Bell et al. discuss the STAR-Vote design. This design is proposed as a potential next-generation electoral system for Travis County and possibly other locations. The authors aim to create a voting system that is secure, transparent, auditable, and reliable. The paper was presented at the 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) in Washington, D.C. by the USENIX Association.

Recent significant technical challenges regarding e-voting systems include, but are not limited to, ensuring secure digital identity management. Every potential citizen must be registered in the electoral system prior to the elections. Their information should be in a format that can be processed digitally. Additionally, their personal identity data should be kept confidential and not shared with any third parties. Traditional e-voting systems may encounter the following issues:

1) Maintaining anonymity in the voting process.
2) Customized ballot procedures for each individual.
3) Verifiability of the ballot only by the voter.
4) High initial costs for setting up the system.
5) Increasing security concerns.
6) Lack of transparency and trust.
7) Voting delays or inefficiencies associated with remote or absentee voting.

III. METHODOLOGY

A. *Proposed Approach*

The design of the suggested approach can be seen in Fig. 1. Our system incorporates blockchain technology. Additionally, there are external entities involved, including:

1) *Election Commission (EC):* The EC is responsible for overseeing the entire election process. It initiates, activates, and closes the election after a specified time. The EC monitors the voting process and releases the results immediately after the election ends. Another crucial task of the EC is to create a voter list before the election through a voter registration process.
2) *Voter:* Individuals who are eligible to vote and are registered in their local election district are known as voters. Each voter has the right to cast a vote for one of the candidates.
3) *Crypto Server:* To ensure the security of votes and maintain privacy, it is necessary to prevent unauthorized access. Every vote is encrypted before being transmitted to the blockchain. To achieve this, a small node server called the crypto server is utilized solely for storing the public and private keys. It does not retain any voting data, and voters do not have access to it.

IV. EXPERIMENTAL

A. *Server Side*

On the server side, there is a blockchain network running with Truffle, Solidity, Ganache, and Node Server components. Truffle is a tool for developing ethereum blockchains, providing features like automation testing, client-side development, network management, and smart contract administration. Solidity is a contract-oriented programming language used to create smart contracts, similar to JavaScript. Ganache is a local blockchain simulator used for managing and testing applications, allowing for safe and secure dApp updates, reusability, and testing without the need for virtual test networks or a remote server.

B. *Client Side*

A user interface has been created for voting with Ethereum accounts on any device, using CSS for design, React JS for data handling, and HTML for markups. Web3.js is used for client-server communication. Metamask is a secure Ethereum wallet that allows users to store, manage, and send Ethers through dApps. It handles public and private keys securely, acting as a bridge between the browser and blockchain network.

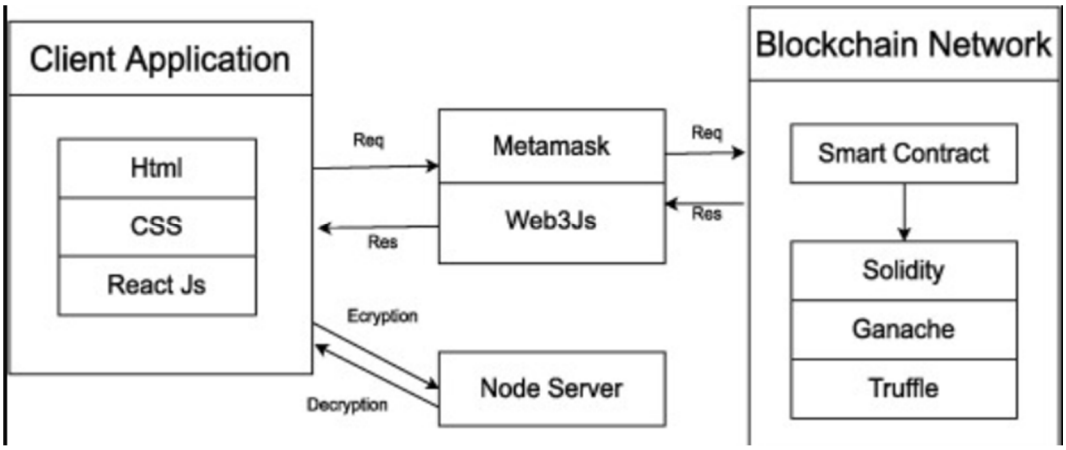


Fig : Architecture

V. CONCLUSION

In the voting system, many countries are facing important uncertainties in ensuring stability. To address this, we have developed a digital voting system that uses blockchain technology and smart contracts. This system aims to ensure the engagement and credibility of voters, the fairness of polling data, and the integrity of vote counting.

Our system operates through three smart contracts that handle various aspects of the election process. This means that the involvement of third parties is minimized compared to other existing systems. Additionally, the votes are encrypted and remain so until the end of the election, ensuring that no one can link a vote to a specific voter.

To further protect voter privacy, we store their information as a hash, making it impossible to identify them within the network. This also reduces costs as only the hash is preserved instead of the full information.

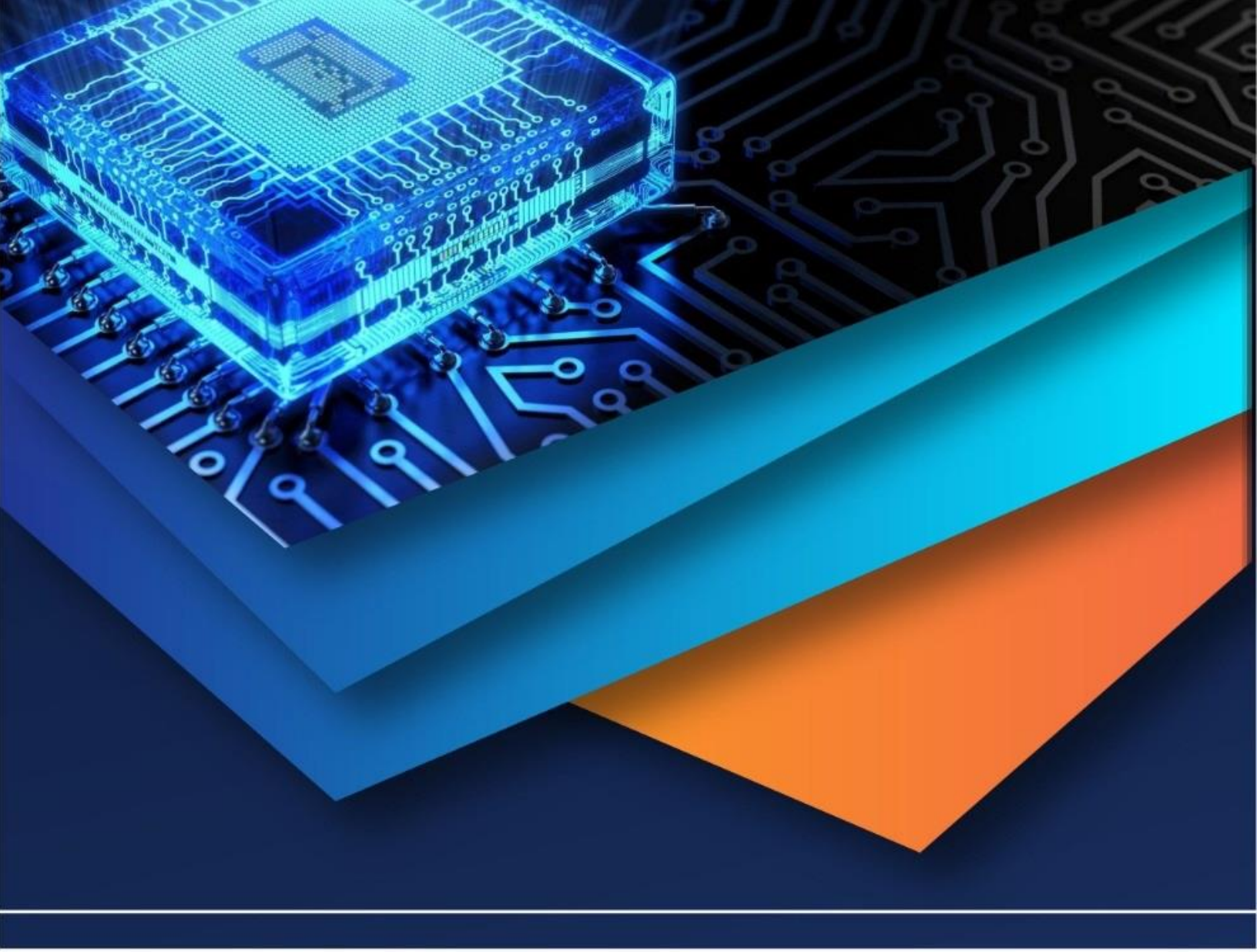
Once the election is over, voters can verify their vote using a unique vote ID that they receive during the voting process. This allows them to confirm that their vote was counted correctly.

By enabling voters to cast their votes using smart devices from anywhere in the world, our system promotes increased voter participation and helps to establish democracy in every region.

In conclusion, our method offers maximum security features such as anonymity, integrity, security, privacy, fairness, verifiability, and mobility, making it a successful option for the election process.

REFERENCES

[1] Adida, B.; ‘Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium
[2] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013)
[3] Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H., 2018, November. Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.
[4] Agbesi, S. and Asante, G., 2019, November. Electronic voting recording system based on blockchain technology. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI) (pp. 1-8). IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY