Voting on ICP Blockchain: A Decentralized Web3 Approach

Mudigonda Dharmateja*
Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada 520007, Andhra Pradesh, India
Email: dharmateja180@gmail.com
*Corresponding Author

Koteswara Rao Kodepogu
Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada 520007, Andhra Pradesh, India
Email: kkrao@pvpsiddhartha.ac.in

Jillela Manoj Kumar
Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada 520007, Andhra Pradesh, India
Email: manojkumarmj991@gmail.com

Muraboina Hari Pavan Gopi Krishna
Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada 520007, Andhra Pradesh, India
Email: krishnamuraboina18@gmail.com

Kodali Ramu
Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada 520007, Andhra Pradesh, India
Email: kodaliramu4@gmail.com

Abstract: In this comprehensive exploration, our paper delves into the intricate implementation of robust authentication and transaction management within the realm of secure voting systems leveraging blockchain technology. Our innovative project stands as a testament to the commitment to privacy and integrity, safeguarding voter interactions through the adept application of advanced cryptographic techniques—all achieved without reliance on a centralized authority. The multifaceted capabilities of blockchain technology are showcased through the seamless facilitation of secure voting processes and the optimization of transaction transfers, collectively contributing to an ecosystem characterized by enhanced security, transparency, and efficiency. Beyond the immediate applications, our study uncovers profound insights into the transformative potential of blockchain within the voting sector, redefining conventional paradigms by introducing unparalleled security measures and transparency to the intricate dynamics of voter interactions. This research not only underscores the feasibility of blockchain in addressing the unique challenges of voting systems but also offers a roadmap for leveraging its capabilities to create a more secure, accountable, and streamlined electoral ecosystem. The paper thus serves as a pioneering contribution, illuminating the path towards a future where blockchain technologies play a pivotal role in shaping the voting landscape.

Index Terms: Internet Computer Blockchain (ICP), Blockchain Voting, Decentralized, Rust, Cryptography, SHA-256 algorithm

1. INTRODUCTION

Democracy and the trustworthiness of electoral processes are crucial for societal stability and prosperity [1]. The core of a democratic ethos lies in transparent, secure, and fair voting systems. Traditional voting methods possess limitations, such as susceptibility to tampering, scalability issues, and transparency concerns. Recent advancements in blockchain technology offer promising solutions to address these challenges.

Blockchain technology, renowned for its decentralized and immutable nature, is reshaping the landscape of voting systems. It holds the potential to establish transparent, secure, and tamper-resistant voting processes. However, despite the considerable potential of blockchain-based e-voting systems, they face criticisms and challenges [2].

Implementing blockchain-based voting systems at the national level, given their inherent complexities and scalability concerns, remains a formidable undertaking [3]. The scale of such elections, combined with the significance of their outcomes, exposes them to interference and security risks. While the adoption of e-voting in various contexts, such as corporate settings, has shown promising results in terms of increased voter turnout and efficiency, these elections can also benefit from more reliable and secure e-voting systems [4].

This paper introduces an innovative approach to corporate voting, specifically focusing on the corporate level. By leveraging the power of blockchain technology, particularly the Internet Computer Protocol (ICP) blockchain, and adopting a decentralized Web3 approach, we propose a secure and innovative e-voting system tailored for the unique requirements of corporate elections. The intention is to draw insights from two key papers in the field.

Our paper outlines the implementation of a decentralized application built on the ICP blockchain, the Corporate Voting system. This system is designed to ensure transparency and anonymity for corporate voters, encompassing two crucial stages: the voting process and subsequent validation. This approach aligns with the evolving landscape of e-voting technologies, offering increased security and efficiency. Through the utilization of blockchain tables and a centralized database, our solution eliminates the need for complex consensus algorithms, enhancing practicality while maintaining privacy and security.

The proposed architecture underscores the separation of layers and roles to prevent undue influence on the voting process. The anonymity of voters and the integrity of the vote are ensured through a unique hash, with no link between voters and their choices stored in the ICP Canisters. This approach upholds the principles of transparency and auditability, devoid of hidden components or potential fraud.

Our aim is to contribute to the ongoing evolution of e-voting systems, particularly in corporate contexts. This paper details the development of a practical and secure e-voting solution for corporate elections, capitalizing on blockchain technology and the decentralized Web3 approach to provide a trustworthy and efficient platform for corporate-level elections.

2. LITERATURE SURVEY

Numerous studies and initiatives have explored the incorporation of blockchain technology into voting systems, aiming to address inherent challenges in traditional voting methods. In this section, we review notable research efforts in this field and highlight their key contributions.

S. S. Hossain et al. emphasize the widespread mistrust in both traditional and digital voting systems, highlighting the necessity for a solution to secure democratic rights. Their proposal introduces a blockchain-based platform to address transparency issues and foster trust between voters and election authorities. The platform incorporates scalable blockchain, flexible consensus algorithms, and a Chain Security Algorithm for enhanced transaction security. The article also discusses smart contracts, encryption methods, and measures against a 51% attack on the blockchain, showcasing the potential for large-scale implementation through performance evaluation [1].

B. Shahzad et al. tackle the shortcomings of electronic voting systems by suggesting a framework that employs effective hashing techniques for enhanced security. The concept of block creation and sealing is introduced, allowing the blockchain to adapt to the polling process. The use of a consortium blockchain, owned by a governing body like the election commission, is

proposed to prevent unauthorized access. The framework aims to improve the security and data management challenges in electronic voting, presenting an advanced manifestation of the process [2].

F. P. Hjálmarsson et al. address the challenge of creating a secure electronic voting system that balances fairness, privacy, transparency, and flexibility. Their focus is on implementing a distributed electronic voting system using blockchain as a service. The paper proposes a novel blockchain-based e-voting system, addressing limitations in existing systems, and evaluates popular blockchain frameworks. A case study on the election process demonstrates how the implementation of a blockchain-based application enhances security and reduces the cost of hosting nationwide elections [3].

N. Mohd. Suki et al. investigate the determinants influencing students' decision-making and satisfaction in campus e-voting, utilizing self-administered questionnaires among university students with past electronic voting experience. Using the PLS-SEM approach, the study identifies voters' commitment as the strongest determinant of decision-making and satisfaction in campus e-voting. High satisfaction is linked to students' commitment and the university's voting requirement, with compulsory voting seen as beneficial for campus development [4].

M. A. Specter et al. scrutinize claims suggesting that "voting over the Internet" or "voting on the blockchain" would enhance election security, finding them misleading. They emphasize the heightened risk of undetectable, nation-scale election failures with Internet- and blockchain-based voting. While online voting may seem convenient, studies suggest it may not significantly increase turnout and could exacerbate disenfranchisement. The article underscores persistent security risks in electronic voting, including blockchain-based systems, and highlights the need for a critical assessment of security in new voting system proposals [5].

The current state of blockchain-based voting systems reveals multiple endeavors aiming to create secure, efficient, and transparent voting mechanisms. However, a comprehensive solution encompassing all these requirements has yet to be realized.

3. GAPS IN LITERATURE

Numerous studies have investigated the incorporation of blockchain technology into voting systems, yet notable gaps persist in the current body of literature, which our paper seeks to fill. While previous research proposed a conceptual architecture for university-level e-voting, it predominantly relied on centralized databases for vote storage and management. Although effective in certain scenarios, this approach fails to fully exploit the potential of blockchain technology within voting systems.

In contrast, our paper advocates a decentralized strategy utilizing the Internet Computer Protocol (ICP) blockchain. The decentralized nature of the ICP blockchain offers considerable advantages. Our Decentralized Application (Dapp) is deployed within an ICP blockchain canister, accessible through HTTP requests and responses, eliminating the necessity for a centralized authority or intermediary entities commonly involved in blockchain voting systems.

A key contribution of our paper lies in eliminating intermediaries during the practical implementation of the voting system. Through the use of the ICP blockchain, we establish a trustless environment where votes are securely recorded and counted without relying on external entities. This not only boosts transparency but also mitigates the risk of manipulation, as the blockchain's immutability ensures the integrity of the voting process.

In summary, existing literature predominantly leans on centralized databases, introducing vulnerabilities and limitations in digital voting systems. Our paper bridges this gap by presenting a decentralized approach utilizing the ICP blockchain, removing intermediaries and bolstering the security, transparency, and scalability of the voting process. This contribution marks a significant advancement in the realm of blockchain-based voting systems.

4. PROPOSED SYSTEM

The envisioned system seeks to transform traditional voting methods by leveraging the unique capabilities of the Internet Computer Protocol (ICP) blockchain. By harnessing the decentralized nature and immutability of the ICP blockchain, the proposed system aims to create a voting process that is secure, efficient, and transparent. This innovative blockchain-based voting system is crafted to address the significant challenges inherent in traditional voting systems, promising a resilient and trustworthy electoral process.

4.1 Voting System Architecture

The architecture of our innovative voting system commences with a user-friendly interface developed using React Admin. Participants can effortlessly log in to the system, ensuring a smooth and intuitive voting experience. What sets our system apart is the implementation of robust security measures for user verification. Each user undergoes verification using SHA-256 cryptography, ensuring the integrity of their identity and preventing unauthorized access. This cryptographic layer adds an additional level of security, crucial for maintaining trust and integrity in the voting process.

Upon successful verification, participants gain access to the Decentralized Application (Dapp) hosted on the Internet Computer Protocol (ICP) blockchain's canister. This Dapp serves as the core component of our system, facilitating the entire voting process through HTTP requests and responses. Utilizing the ICP blockchain, data updates are stored in respective canisters distributed across the system, ensuring data integrity and availability. An integral aspect of our architecture is the utilization of the Rust programming language, known for its reliability and performance in smart contract development. The use of Rust streamlines the creation of secure and efficient smart contracts, ensuring that votes are accurately recorded and counted, making our voting system both secure and reliable.

This architecture seamlessly integrates user-friendly interfaces, strong cryptography, blockchain technology, and Rust programming language for smart contract development, culminating in a comprehensive and trustworthy voting system for corporate participants.

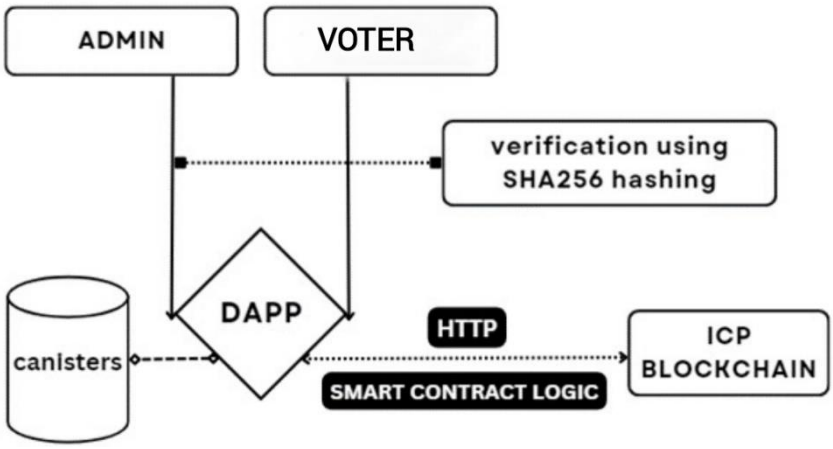


Fig. 1. Voting System Architecture

4.2 Workflow of the Proposed Model

4.2.1 Decision Proposal
- The administrative staff (Admin) proposes decisions with a set of voting options.

4.2.2 Voting Process
- Voters actively participate by casting their votes on the available decisions.
- To cast a vote, voters should have a of token in their account.
- When a voter casts a vote, tokens is deducted from their account.
- The system ensures that tokens cannot be shared to other voters.

4.2.3 Vote Counting
- The Admin can access the system to view the number of votes cast for each option within a specific decision.
- The voting system keeps a tally of the votes for each option.

4.2.4 Decision Making
- When the voting period concludes or at the discretion of the Admin, the system determines the option with the majority of votes for each decision.
- The option with the most votes is declared the winner.
- After a decision is made, the voting data can be safely stored in the canister.

4.2 System Advantages

Our proposed system distinguishes itself by leveraging the inherent immutability of blockchain technology. This feature renders the entire voting process resistant to tampering, providing a secure defense against any potential single point of failure. Key advantages of the proposed system include:

- Transparency: All transactions are meticulously recorded and accessible on the blockchain, affording voters a clear and transparent view of the voting process.

- Security: Employing cryptographic hashing, secure networks, and robust consensus algorithms, the system significantly mitigates the risk of intrusion.

- Efficiency: The adaptability of consensus algorithms and smart contracts optimizes the system's efficiency, guaranteeing accurate and timely vote counting.

- Accessibility: Voters enjoy the convenience of participating from any location worldwide, while the system preserves the integrity of their votes.

- Trust: Through end-to-end verification, our system enhances voter trust, ensuring that voters maintain confidence in the entire voting process.

Our proposed system presents a comprehensive solution to the challenges encountered by both traditional and digital voting systems. It harmonizes the advantages of blockchain technology with a flexible and adaptable architecture, resulting in a highly secure, efficient, and transparent voting management system.

5. TECHNOLOGIES USED

5.1 Internet Computer Protocol Blockchain

The Internet Computer Protocol (ICP) serves as a communication protocol utilized for transmitting data across the internet. This dependable and connection-oriented protocol allows applications to establish, maintain, and terminate connections between devices. On the other hand, Blockchain serves as a decentralized and distributed ledger technology created to enable the secure, transparent, and immutable recording of transactions. While commonly associated with cryptocurrencies like Bitcoin, Blockchain finds utility in various sectors such as supply chain management and voting systems. Despite sharing certain similarities, these technologies differ in their intended purposes and operational mechanisms.

5.2 Rust Programming Language

The Rust programming language surfaces as a modern and memory-safe language designed for developers venturing into the development of the next generation of distributed applications intended for execution on the Internet Computer blockchain network. Tailored to suit the unique characteristics of the Internet Computer, Rust provides a programming environment that is not only familiar but also robust. As an evolving language, Rust undergoes continuous refinement, embracing support for innovative features and various enhancements.

5.3 React Js

ReactJS is a JavaScript library designed for building user interfaces. Developed initially by Facebook, it is currently under the joint stewardship of Facebook and a collaborative community involving individual developers and various companies. This library provides developers with the capability to create reusable UI components, streamlining the complex task of building dynamic and interactive web applications.

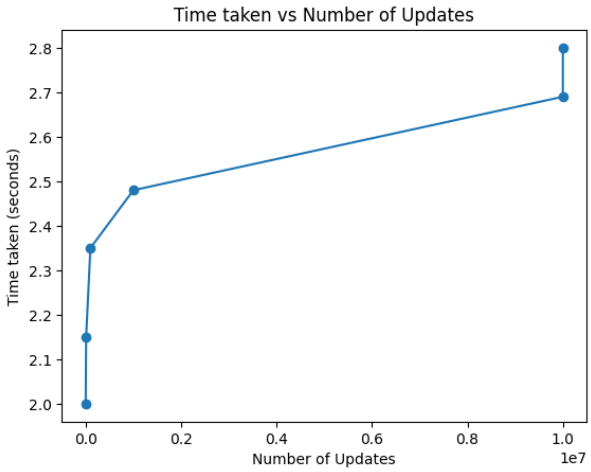
6. PERFORMANCE EVALUATION

In the performance evaluation of our paper, we employ response time as a crucial evaluation metric for our voting system. To provide a comprehensive assessment, we present two key graphs. The first graph illustrates the response time in relation to the number of queries, ranging from 1000 to 10000000. This graph vividly demonstrates how our system handles varying levels of user queries, showcasing its responsiveness. The second graph highlights the relationship between the number of updates, i.e., write operations on the blockchain, and the associated response time, also spanning from 1000 to 10000000. These graphs collectively offer a clear and quantitative representation of our system's performance, emphasizing its efficiency and scalability.

Table 1. Number of Updates and Time taken

S.No	No. of Updates	Time taken(seconds)
1	1000	2.00
2	10000	2.15
3	100000	2.35
4	1000000	2.48
5	10000000	2.69
6	10000000	2.80

Graph 1. Time taken for Updates vs. Number of Updates



As the graph shows, on the x-axis, we have the "Number of Queries," which represents the quantity of interactions or requests made to our DApp. On the y-axis, we have "Time Taken (seconds)," which indicates the amount of time it takes for our DApp to respond to these queries.
Analysis of the performance based on the graph:

1.Consistency: One notable aspect is the consistency in response time. Even as the number of queries increases from 1000 to 10000000, the response time remains relatively stable. This suggests that our DApp maintains a consistent level of performance, which is a positive sign.

2. Scalability: Our DApp seems to handle an increase in the number of queries quite well. The slight increase in response time as the number of queries grows suggests that our system is scalable, which is essential for accommodating more users or transactions in the future.
3. Efficiency: The response times, ranging from 0.030 to 0.050 seconds, indicate that our DApp is responding quickly to user queries.
This efficiency is crucial in providing a smooth and responsive user experience.
4. Reliability: The consistent response times across different query quantities reflect the reliability of our DApp. Users can rely on it to perform consistently, regardless of the workload.

Overall, based on this analysis, our DApp demonstrates good performance in terms of consistency, scalability, efficiency, and reliability. This bodes well for providing users with a seamless and dependable voting experience.

7. CONCLUSION

In conclusion, this project has effectively harnessed the capabilities of blockchain technology and contemporary web development to establish a secure, transparent, and efficient platform aimed at improving governance within corporate settings. Through the utilization of the Internet Computer Protocol (ICP) blockchain, we have achieved an unprecedented level of decentralization and data integrity. This technological advancement empowers corporate stakeholders to actively engage in decision-making processes via a token-based voting system, fostering a culture of participation and responsibility.

The tailored authentication system ensures secure access for both corporate members and administrators, while orthogonal persistence guarantees the immutability of critical corporate data. React, a versatile JavaScript library for crafting user interfaces, contributes to a seamless and responsive user experience. The amalgamation of these components results in a solution that not only promotes corporate excellence but also enables members to contribute effectively to decision-making processes, thereby enhancing the inclusivity and dynamism of corporate governance.

This project exemplifies the potential of combining blockchain and web technologies to transform governance systems in diverse domains. Embracing this innovative approach represents a significant stride towards improving transparency, accountability, and stakeholder participation within corporate structures. In the continually evolving intersection of technology and corporate governance, this project establishes a promising precedent for future advancements.

8.REFERENCES

[1] S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, "E-voting system using blockchain technology," in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 113–117, doi: 10.1145/3376044.3376062.

[2] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[3] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based E-Voting system," in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.

[4] N. Mohd. Suki and N. Mohd. Suki, "Decision-making and satisfaction in campus e-voting: Moderating effect of trust in the system," J. Enterprise Inf. Manage., vol. 30, no. 6, pp. 944–963, Oct. 2017, doi: 10.1108/JEIM-08-2016-0151.

[5] C. Culnane, A. Essex, S. J. Lewis, O. Pereira, and V. Teague, "Knights and knaves run elections: Internet voting and undetectable electoral fraud," IEEE Secur. Privacy, vol. 17, no. 4, pp. 62–70, Jul. 2019, doi: 10.1109/MSEC.2019.2915398.

[6] M. A. Specter, J. Koppel, and D. Weitzner, "The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting application used in U.S. federal elections," in Proc. 29th USENIX Secur. Symp., 2020, pp. 1535–1552.