International Journal of Safety and Security Engineering
Vol. 14, No. 1, February, 2024, pp. 91-98
Journal homepage: http://iieta.org/journals/ijsse

Student Voting on ICP Blockchain: A Decentralized Web3 Approach-An Infrastructure Protection System

Koteswara Rao Kodepogu*, Mudigonda Dharmateja, Jillela Manoj Kumar, Muraboina Hari Pavan Gopi Krishna, Kodali Ramu

CSE Department, PVP Siddhartha Institute of Technology, Vijayawada 520007, India

Corresponding Author Email: kkrao@pvpsiddhartha.ac.in

https://doi.org/10.18280/ijsse.140109

Received: 29 November 2023
Revised: 26 January 2024
Accepted: 12 February 2024
Available online: 29 February 2024

Keywords:
ICP, student voting, decentralized, consensus, cryptography, encryption, SHA-256 algorithm

ABSTRACT

In this exploration, our paper delves into the intricate implementation of robust authentication and transaction management within educational blockchain systems. Our project showcases a commitment to privacy and integrity, safeguarding interactions through advanced cryptographic techniques. The multifaceted capabilities of blockchain technology are showcased through the seamless maintenance of student records, the facilitation of secure voting processes, and the optimization of token transfers, collectively contributing to an ecosystem characterized by enhanced security, transparency, and efficiency. Our study uncovers insights into blockchain's transformative potential in education, redefining paradigms by introducing security measures and transparency to student-admin interactions. We highlight the successful implementation of blockchain-based authentication and transaction management systems, leading to enhanced educational processes. Additionally, we briefly outline our research design and methodology, emphasizing the rigorous approach to exploring blockchain applications.

1. INTRODUCTION

Democracy and trust in electoral processes are fundamental to the stability and prosperity of any society [1]. Transparent, secure, and equitable voting systems are at the heart of this democratic ethos. Traditional voting methods have their limitations, including the potential for tampering, scalability issues, and concerns related to transparency [2]. Recent developments in blockchain technology have presented promising solutions to address these challenges [2].

This paper presents a pioneering approach by leveraging blockchain technology, specifically the Internet Computer Protocol (ICP) blockchain, to revolutionize student voting systems. By adopting a decentralized Web3 approach, our proposed e-voting system offers unprecedented transparency, security, and scalability. It offers the potential to create transparent, secure, and tamper-resistant voting processes [2]. However, while blockchain-based e-voting systems have shown immense potential, they have also faced their share of criticisms and challenges [2].

At the national level, implementing blockchain-based voting systems, with their inherent complexities and scalability concerns, remains a formidable task [3]. The scale of such elections, coupled with the significance of their outcomes, makes them vulnerable to interference and security risks. While the adoption of e-voting in universities has shown promising results in terms of increased voter turnout and efficiency [4], university-level elections can also benefit from more reliable and secure e-voting systems [4].

The primary goal of this paper is to introduce a novel approach to student voting, with a specific focus on the university level. Our aim is to address the challenges associated with traditional voting methods by proposing an innovative e-voting system tailored for student elections. Leveraging the power of blockchain technology, specifically the Internet Computer Protocol (ICP) blockchain, and adopting a decentralized Web3 approach, we propose an innovative and secure e-voting system tailored for the unique needs of student elections. In this context, we aim to draw upon the valuable insights from two key papers in the field.

Our paper introduces a decentralized application built on the ICP blockchain, known as the Student Voting system. This system is designed to ensure transparency and anonymity for student voters and consists of two essential stages: the voting process itself and the subsequent validation. This approach aligns with the evolving landscape of e-voting technologies, offering increased security and efficiency. By utilizing 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 emphasizes separation of layers and roles to prevent any undue influence on the voting process. A unique hash ensures the anonymity of voters while guaranteeing the integrity of the vote, with no link between voters and their choices stored in the ICP Canisters. With this approach, we uphold the principles of transparency and auditability, free from hidden components or potential fraud.

We aim to contribute to the ongoing evolution of e-voting systems, particularly in university contexts. This paper outlines the development of a practical and secure e-voting solution for students, taking advantage of blockchain technology and the decentralized Web3 approach to provide a trustworthy and efficient platform for university-level elections.

2. LITERATURE SURVEY

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

Oprea et al. [1] introduced a digital voting system leveraging blockchain technology for implementation in technologically advanced environments. While their system assumed the trustworthiness of external entities, it acknowledged the security vulnerabilities associated with this approach. The practical implication of this finding is the recognition of the importance of implementing stringent authentication and authorization protocols to safeguard the integrity of voting systems against external threats.

Farooq et al. [2] presented a system that aimed to make the voting system transparent using blockchain technology. However, their approach raised questions about the transparency of the system itself.

Chang et al. [3] reviewed the past, present, and future of global health financing, highlighting the importance of financial structures. However, this work is not directly related to blockchain-based voting systems and their challenges.

Hossain et al. [4] developed an e-voting system using blockchain technology but didn't address the issue of voter privacy and complex computations.

Shahzad and Crowcroft [5] proposed trustworthy electronic voting using adjusted blockchain technology, focusing on security aspects. The practical implication is the adoption of cryptographic primitives such as digital signatures and hash functions to provide end-to-end verifiability and integrity assurance in electronic voting protocols.

Hjálmarsson et al. [6] introduced a blockchain-based e-voting system but didn't address issues related to voter identity and voter verification. In our proposed system, we streamline the verification process and enhance voter trust using registered student IDs [1], thus improving security and transparency.

Suki and Suki [7] studied decision-making and satisfaction in campus e-voting systems, emphasizing trust in the system.

Culnane et al. [8] discussed undetectable electoral fraud in internet voting systems, emphasizing the security challenges. Our proposed system leverages the ICP blockchain's security and transparency, providing a solution to some of these challenges.

Specter et al. [9] conducted a security analysis of Voatz, an internet voting application. Our research can build upon this by incorporating robust security measures inspired by Specter et al.'s findings to enhance the resilience of our blockchain-based voting system against cyber threats and attacks.

Lewis and Rice [10] studied voter turnout in undergraduate student government elections but did not address blockchain-based voting systems. The practical implication here is the recognition of the need to design voting systems that not only ensure security and transparency but also actively engage and encourage voter participation.

Haines et al. [11] explored methods for proving election outcomes but did not directly relate to blockchain-based voting systems. By incorporating verifiability features, our proposed blockchain-based voting system can provide voters and stakeholders with greater confidence in the accuracy and legitimacy of election results.

Albertson and Guiler [12] focused on conspiracy theories, election rigging, and support for democratic norms, which, while important, were not directly related to blockchain-based voting systems.

Shah et al. [13] discussed the Block Chain Voting System but did not address the specific challenges and contributions of blockchain-based voting systems.

Chaum et al. [14] presented an end-to-end voter-verifiable optical-scan voting system, emphasizing verifiability. In our proposed system, we streamline the verification process, enhancing voter trust through registered student IDs [1], making the voting system more secure and transparent.

McCorry et al. [15] developed a smart contract for boardroom voting, focusing on maximum voter privacy. The practical implication of their work is the recognition of the need to integrate strong privacy protections into blockchain-based voting protocols to safeguard voter confidentiality and prevent unauthorized access to sensitive voting data.

Pawlak et al. [16] worked towards intelligent agents for a blockchain e-voting system, emphasizing the role of technology in the voting process.

Fusco et al. [17] introduced Crypto-voting, a blockchain-based e-voting system. By incorporating design principles and security features inspired by Crypto-voting, our proposed blockchain-based voting system can provide a robust and trustworthy platform for conducting elections.

The current landscape of blockchain-based voting systems reveals that while several endeavors have aimed to create secure, efficient, and transparent voting mechanisms, a comprehensive solution encompassing all these requirements has yet to be realized.

Park et al. [18] explained about how can, "Going from bad to worse: From internet voting to block chain voting in all aspects.

Khan et al. [19] explained about "Secure digital voting system based on block chain technology" in all aspects.

Adiputra et al. [20] explained about “A proposal of block chain based electronic voting system," in all aspects.

3. GAPS IN LITERATURE

While various studies have explored the integration of blockchain technology into voting systems, there are distinct gaps in the existing literature that your paper aims to address. Notably, the majority of previous research, suggested a conceptual architecture for e-voting at the university level was presented, but it primarily relied on a centralized database for vote storage and management. While this approach may work in certain scenarios, it falls short of leveraging the full potential of blockchain technology, particularly in the context of voting systems.

In contrast, our paper offers a decentralized approach that leverages the Internet Computer Protocol (ICP) blockchain. The decentralized nature of the ICP blockchain brings significant advantages to the forefront. By deploying our project within the ICP blockchain, our Decentralized Application (Dapp) runs in a canister, accessible through HTTP requests and responses. This eliminates the need for a centralized authority or intermediary entities that are traditionally involved in blockchain voting systems.

One of the key contributions of our paper is the removal of intermediaries in the practical implementation of the voting system. By utilizing the ICP blockchain, we establish a trustless environment where votes are securely recorded and counted without the need for trust in external entities, as opposed to systems relying on centralized databases. This not only enhances transparency but also minimizes the risk of manipulation, as the immutability of the blockchain ensures the integrity of the voting process. Moreover, a comparative analysis highlights that while centralized databases introduce vulnerabilities and limitations in digital voting systems, our decentralized approach offers inherent advantages in terms of security, transparency, and scalability.

Furthermore, while previous research, including the study of Oprea et al. [1], encountered challenges in terms of scalability and voter privacy, our proposed system addresses these concerns. Recent studies have highlighted the limitations of traditional blockchain-based voting systems in managing large-scale elections and ensuring voter privacy. The ICP blockchain's built-in consensus mechanism and cryptographic hashing optimize latency, ensuring efficient management of a large number of voters. The blockchain's decentralization and immutability strengthen user trust, addressing the limitations found in centralized databases.

In summary, the existing literature primarily relies on centralized databases, introducing vulnerabilities and limitations in digital voting systems. Our paper bridges this gap by offering a decentralized approach that leverages the ICP blockchain, eliminating intermediaries and enhancing the security, transparency, and scalability of the voting process. This contribution represents a significant step forward in the field of blockchain-based voting systems.

4. PROPOSED SYSTEM

The proposed system aims to revolutionize the conventional voting methods by harnessing the exceptional capabilities of the Internet Computer Protocol (ICP) blockchain. It utilizes the decentralized nature and immutability of the ICP blockchain to establish a secure, efficient, and transparent voting process. This blockchain-based voting system is designed to overcome the critical challenges associated with traditional voting systems, ensuring a resilient and trustworthy electoral process.

4.1 Voting system architecture

The architecture of our innovative voting system begins with a user-friendly interface developed using React Admin. Students can effortlessly log in to the system, facilitating a seamless and intuitive voting experience. What sets our system apart is the robust security measures implemented for user verification. Each user is verified using SHA-256 cryptography, ensuring the integrity of their identity and preventing unauthorized access. This cryptographic layer adds an extra dimension of security, crucial for maintaining the trust and integrity of the voting process.

Once verified, students gain access to the Decentralized Application (Dapp) hosted on the Internet Computer Protocol (ICP) blockchain's canister. This Dapp is the core component of our system, facilitating the entire voting process through HTTP requests and responses. By harnessing the power of the ICP blockchain, updates and data are securely stored across distributed canisters, ensuring both the integrity and availability of critical information. An essential element of our architecture is the use of the Motoko programming language, the built-in language for ICP's smart contract development. The adoption of Motoko streamlines the creation of secure and efficient smart contracts, ensuring the precise recording and tallying of votes, thus cementing the reliability of our voting system.

This architecture combines user-friendly interfaces, strong cryptography, blockchain technology, and smart contract development, creating a comprehensive and trustworthy voting system for students. The architecture of the student voting can be seen in Figure 1.

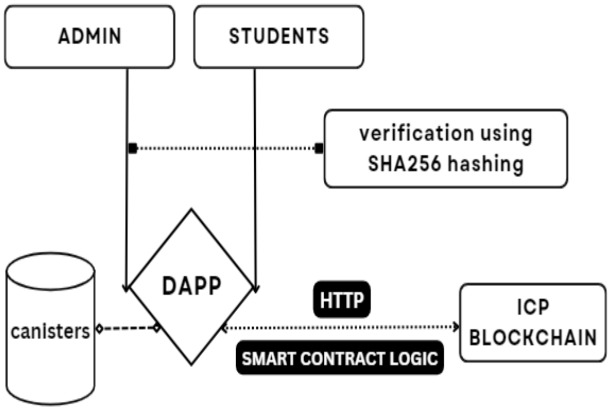


Figure 1. Student voting system architecture

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

Students actively participate by casting their votes on the available decisions.

To cast a vote, students should have a minimum number of tokens in their account.

When a student casts a vote, a constant amount of tokens are deducted from their account.

The system ensures that students cannot vote again for the same decision.

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 for that particular decision can be cleared from memory.

4.3 System advantages

Our proposed system stands out by capitalizing on the immutability of blockchain technology. This makes the entire voting process resistant to tampering and secure against any single point of failure. Notable advantages of the proposed system include:

- Transparency: Every transaction is recorded and accessible on the blockchain, providing voters with a transparent view of the voting process.

- Security: Through cryptographic hashing, secure networks, and robust consensus algorithms, the system minimizes the risk of intrusion.

- Efficiency: The flexibility of consensus algorithms and smart contracts optimize the system's efficiency, ensuring that votes are counted accurately and in a timely manner.

- Accessibility: Voters can participate from anywhere in the world, and the system maintains the integrity of their votes.

- Trust: By enhancing voter trust through end-to-end verification, our system ensures that voters have confidence in the voting process.

Our proposed system offers a comprehensive solution to the challenges faced by traditional and digital voting systems. It combines the benefits of blockchain technology with a flexible and adaptable architecture to create a highly secure, efficient, and transparent voting management system.

5. TECHNOLOGIES USED

5.1 Internet computer protocol blockchain

The Internet Computer Protocol (ICP) functions as a communication protocol employed for the transmission of data across the internet. This reliable and connection-oriented protocol enables applications to initiate, sustain, and conclude connections between devices. ICP is integral to the functioning of the Internet Computer blockchain network, providing the underlying communication infrastructure. In contrast, Blockchain stands as a decentralized and distributed ledger technology designed to facilitate the secure, transparent, and immutable documentation of transactions. Although frequently utilized in cryptocurrencies like Bitcoin, Blockchain finds application in diverse sectors such as supply chain management and voting systems. While there are certain parallels between them, these technologies diverge in their intended functions and operational mechanisms. These technologies work in tandem, with ICP enabling efficient data transmission and Blockchain ensuring secure and transparent transaction recording.

5.2 Motoko programming language

The Motoko programming language emerges as a contemporary and type-safe language tailored for developers aspiring to construct the forthcoming wave of distributed applications intended for execution on the Internet Computer blockchain network. Specifically crafted to accommodate the distinctive attributes of the Internet Computer, Motoko furnishes a programming environment that is both familiar and resilient. In its capacity as a nascent language, Motoko undergoes continual refinement, incorporating support for novel features and various enhancements. While other languages like Rust and JavaScript could have been used, Motoko was chosen for its seamless integration with the Internet Computer's architecture and its ability to handle the unique demands of distributed computing.

5.3 ReactJS

ReactJS stands as a JavaScript library dedicated to constructing user interfaces. Originating from the labs of Facebook, it currently undergoes joint stewardship by Facebook itself and a collaborative community comprising individual developers and various companies. This library empowers developers in crafting reusable UI components, thereby simplifying the intricate process of constructing dynamic and interactive web applications. ReactJS was chosen over alternatives like Angular and Vue.js due to its efficient virtual DOM implementation and the flexibility it offers developers in managing application state.

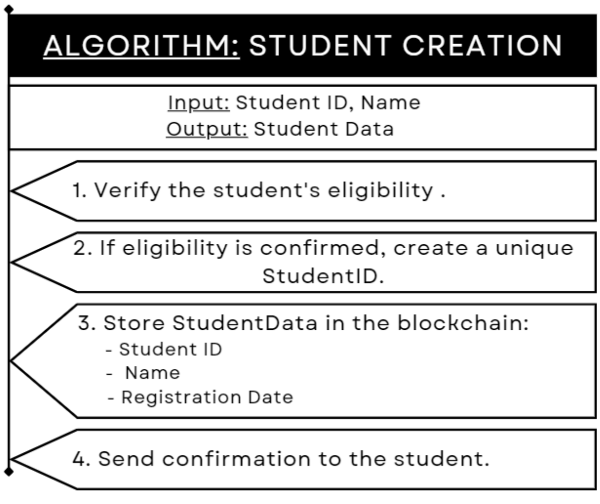
6. DESIGN AND IMPLEMENTATION

In this section, we present the design and implementation details of our blockchain-based voting system. Our system leverages the Internet Computer Protocol (ICP) blockchain and a React-based frontend to provide a secure and user-friendly voting platform. We describe the algorithms for student creation, casting votes, secure login, and additional critical functionalities. We also discuss how the system handles exceptions or errors and its scalability.

6.1 Algorithms

6.1.1 Student account creation

The student creation algorithm allows eligible students to register for voting. Students are verified against the Canister data (ICP Blockchain decentralized data storage unit) before they can participate in the voting process. In case of exceptions or errors, such as a student trying to register with an already registered StudentID, the system throws an error message and prompts the student to try again with a different ID. The caption of the student voting can be seen in Figure 2.



ALGORITHM: STUDENT CREATION

Input: Student ID, Name
Output: Student Data

1. Verify the student's eligibility .

2. If eligibility is confirmed, create a unique StudentID.

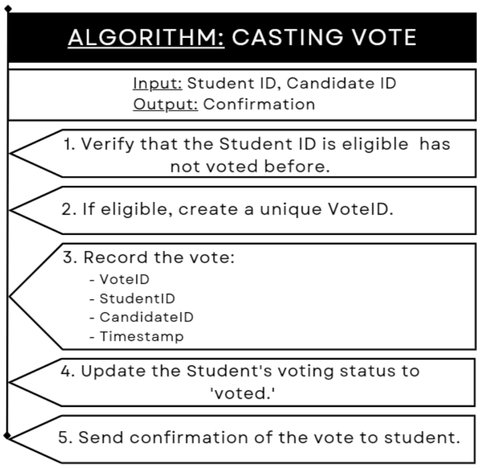
3. Store StudentData in the blockchain:
- Student ID
- Name
- Registration Date

4. Send confirmation to the student.

Figure 2. Caption of student voting

6.1.2 Cast vote

The casting vote algorithm records a student's vote and ensures that they can only vote once. If a student tries to vote more than once, the system throws an error. The process of casting vote can be seen in Figure 3.



ALGORITHM: CASTING VOTE

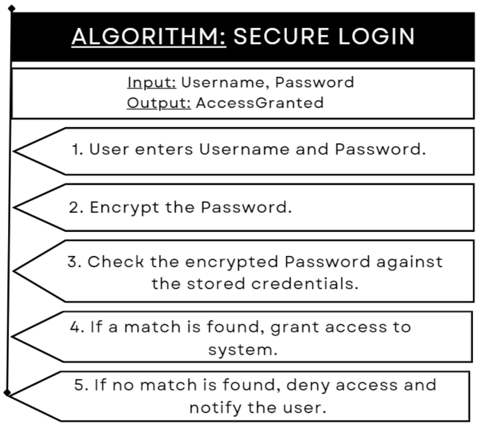
Input: Student ID, Candidate ID
Output: Confirmation

1. Verify that the Student ID is eligible has not voted before.
2. If eligible, create a unique VoteID.
3. Record the vote:
   - VoteID
   - StudentID
   - CandidateID
   - Timestamp
4. Update the Student's voting status to 'voted.'
5. Send confirmation of the vote to student.

Figure 3. Casting vote

6.1.3 Secure login

The secure login algorithm ensures that only authorized users gain access to the system, preventing unauthorized access. If a user enters incorrect login credentials, the system throws an error and prompts the user to try again. The secure login can be seen in Figure 4.



ALGORITHM: SECURE LOGIN

Input: Username, Password
Output: AccessGranted

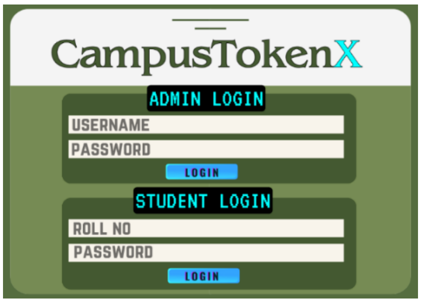
1. User enters Username and Password.
2. Encrypt the Password.
3. Check the encrypted Password against the stored credentials.
4. If a match is found, grant access to system.
5. If no match is found, deny access and notify the user.

Figure 4. Secure login

6.2 System workflow

6.2.1 User login

- Students register using their StudentID.
- Eligible students are assigned a unique StudentID.
- Student data is stored in the blockchain. The system is designed to handle a large number of student registrations, ensuring scalability. The User login can be seen Figure 5.



CampusTokenX

ADMIN LOGIN

USERNAME

PASSWORD

LOGIN

STUDENT LOGIN

ROLL NO

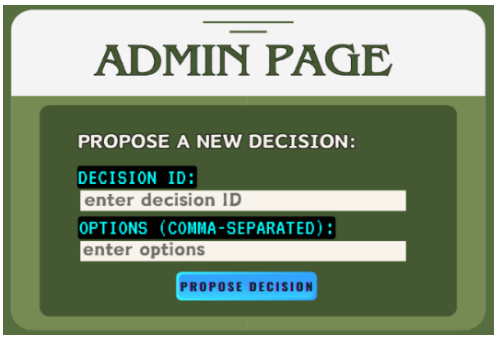
PASSWORD

LOGIN

Figure 5. User login

6.2.2 Create decision

- Admin proposes a decision and provides options for which students have to participate.
- Decision ID specifies the decision and options for that decision should be entered in Options input, they should be separated using commas. The system can handle multiple decisions and options, demonstrating its scalability. The process of create decision can be seen Figure 6.



ADMIN PAGE

PROPOSE A NEW DECISION:

DECISION ID: enter decision ID

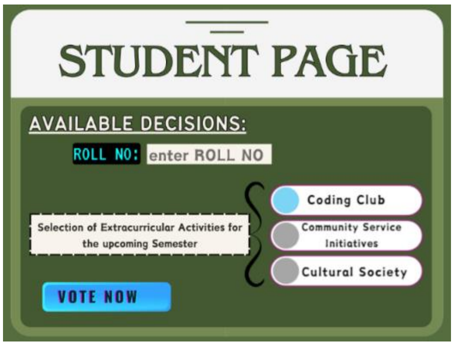
OPTIONS (COMMA-SEPARATED): enter options

PROPOSE DECISION

Figure 6. Creating decision

6.2.3 Student voting

- Eligible students cast their votes using their StudentID.
- Votes are recorded on the blockchain, ensuring transparency and immutability. The system is capable of recording a large number of votes, further demonstrating its scalability. The Process of Choosing the options can be seen in Figure 7.



STUDENT PAGE

AVAILABLE DECISIONS:

ROLL NO: enter ROLL NO

Selection of Extracurricular Activities for the upcoming Semester

○ Coding Club
○ Community Service Initiatives
○ Cultural Society

VOTE NOW

Figure 7. Choosing options for a decision

7. PERFORMANCE EVALUATION

In the performance evaluation of our paper, we employ response time as a crucial evaluation metric for our voting system. Our testing environment simulated a network of 1000 nodes to mimic real-world conditions. 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 1 to 1000. 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 1 to 1000. These graphs collectively offer a clear and quantitative representation of our system's performance, emphasizing its efficiency and scalability.

We also tested our system under adverse conditions, such as network outages and data corruption scenarios. Our system demonstrated resilience by recovering and continuing operation without significant impact on response times. The number of updates and time taken seen in Table 1.

Table 1. Number of updates and time taken

S. No.	No. of Updates	Time Taken (Seconds)
1	1	2.10
2	10	2.15
3	100	2.20
4	250	2.25
5	500	2.30
6	1000	2.35

Table 2. Number of queries and time taken

S. No.	No. of Queries	Time Taken (Seconds)
1	1	0.026
2	10	0.026
3	100	0.026
4	250	0.027
5	500	0.028
6	1000	0.029

As Figure 8 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 thegraph:

1. **Consistency**: One notable aspect is the consistency in response time. Even as the number of queries increases from 1 to 1000, 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 0.026 to 0.029 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.

The number of queries and time taken can be seen in Table 2.

In Figure 9:

- On the x-axis, we have "Number of Updates," representing the quantity of updates or changes made to our DApp.

On the y-axis, we have "Time Taken (seconds)," indicating the time it takes for our DApp to process these updates.

Analysis of the performance based on the graph:

1. **Incremental Time Increase**: As the number of updates increases, we can observe a gradual and incremental increase in the time taken for these updates. This suggests that our DApp's performance remains relatively stable as the update load grows. The increase in processing time is consistent and predictable.

2. **Predictable Scalability**: The predictable and incremental nature of the time increase indicates that our DApp is scalable. It can accommodate additional updates without experiencing sudden spikes in processing time, which is vital for maintaining a smooth user experience during periods of high activity.

3. **Consistency**: The performance of our DApp is consistent, which is a positive sign for users. They can expect a uniform experience regardless of the number of updates, as there are no sudden spikes or dips in processing time.

4. **Stability**: The stable and gradual increase in processing time suggests that our DApp is stable and capable of handling a growing number of updates without causing disruptions.

In summary, this analysis indicates that our DApp exhibits consistent and predictable performance when dealing with various numbers of updates. It demonstrates scalability, maintaining stable processing times as the update load increases. This reliability ensures that users can rely on our DApp for efficient and consistent interactions, which is crucial for the success of a voting application.

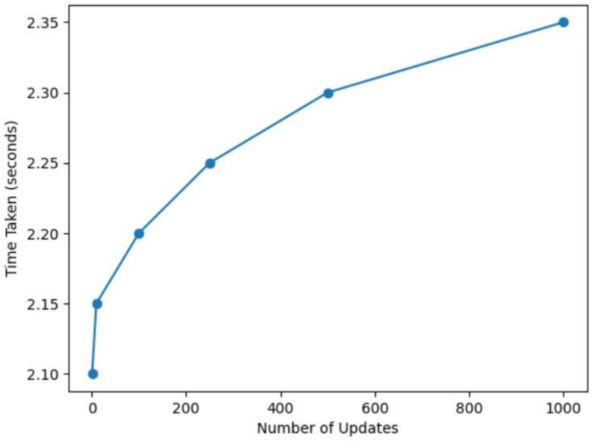


Figure 8. Time taken for updates vs. number of updates

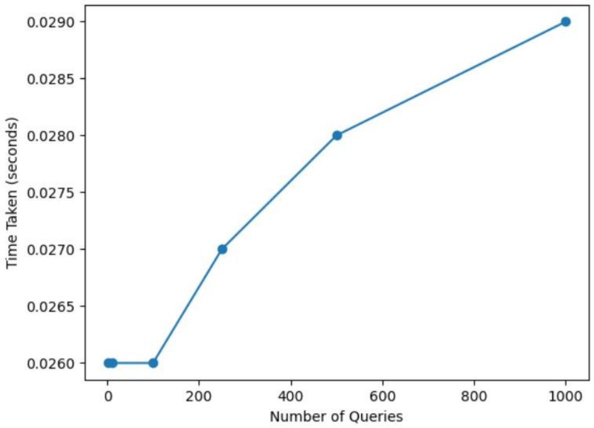


Figure 9. Time taken for queries vs. number of queries

8. CONCLUSIONS

In conclusion, this project has successfully leveraged the power of blockchain technology and modern web development to create a secure, transparent, and efficient platform for enhancing governance within educational institutes. By utilizing the Internet Computer Protocol (ICP) blockchain, we have achieved an unprecedented level of decentralization and data integrity. This technology has empowered students to actively participate in decision-making through a token-based voting system, thereby fostering a culture of involvement and accountability.

The custom authentication system ensures that students and administrators can securely access the platform, while orthogonal persistence guarantees that vital student data remains tamper-proof. React, a versatile JavaScript library for building user interfaces, has provided a seamless and responsive user experience. The integration of these elements has culminated in a solution that promotes academic excellence and empowers students to contribute to extracurricular activities, making governance within educational institutes more inclusive and dynamic.

As this project demonstrates, the convergence of blockchain and web technologies holds immense potential for revolutionizing governance systems across various domains. By embracing this innovative approach, we have taken a significant step towards enhancing transparency, accountability, and student participation in educational institutions, which are the cornerstones of effective governance. In the ever-evolving landscape of technology and education, this project sets a promising precedent for the future.

9. FUTURE WORK

The blockchain-based decentralized voting system designed for educational institutes, as presented in this report, marks a significant advancement in the modernization and security of the voting process. Nevertheless, several avenues for potential future work and enhancements are identified. Firstly, it is imperative to focus on enhancing the system's security through continuous research, vulnerability assessment, and the development of robust countermeasures. Secondly, optimizing the user experience (UX) by conducting user studies and feedback analysis will ensure an intuitive and user-friendly interface. Thirdly, exploring methods to seamlessly integrate the decentralized voting system with existing educational platforms can provide a more comprehensive solution. Additionally, adapting the system for mobile accessibility, including the development of mobile applications, can cater to users who prefer voting via smartphones or tablets. Finally, it is essential to remain abreast of blockchain advancements, particularly within the ICP ecosystem, and evaluate how these innovations can be integrated to augment the system's capabilities. These ongoing efforts reflect the commitment to continually enhance and expand the blockchain-based decentralized voting system for educational institutes, ensuring it remains adaptable to the evolving needs and expectations of educational institutions and their voting processes.

REFERENCES

[1] Oprea, S.V., Bâra, A., Andreescu, A.I., Cristescu, M.P. (2023). Conceptual architecture of a blockchain solution for e-voting in elections at the university level. IEEE Access, 11: 18461-18474. https://doi.org/10.1109/ACCESS.2023.3247964

[2] Farooq, M.S., Iftikhar, U., Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. IEEE Access, 10: 59959-59969. https://doi.org/10.1109/ACCESS.2022.3180168

[3] Chang, A.Y., Cowling, K., Micah, A.E., Chapin, A., Chen, C.S., Ikilezi, G., Qorbani, M. (2019). Past, present, and future of global health financing: A review of development assistance, government, out-of-pocket, and other private spending on health for 195 countries, 1995–2050. The Lancet, 393(10187): 2233-2260. https://doi.org/10.1016/S0140-6736(19)30841-4

[4] Hossain, S.S., Arani, S.A, Rahman, M.T., Bhuiyan, T., Alam, D., Zaman, M. (2019). E-voting system using blockchain technology. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, New York, NY, USA, pp. 113-117. https://doi.org/10.1145/3376044.3376062

[5] Shahzad, B., Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7: 24477-24488. https://doi.org/10.1109/ACCESS.2019.2895670

[6] Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M., Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986. https://doi.org/10.1109/CLOUD.2018.00151

[7] Suki, N.M., Suki, N.M. (2017). Decision-making and satisfaction in campus e-voting: Moderating effect of trust in the system. Journal of Enterprise Information Management, 30(6): 944-963. https://doi.org/10.1108/JEIM-08-2016-0151

[8] Culnane, C., Essex, A., Lewis, S.J., Pereira, O., Teague, V. (2019). Knights and knaves run elections: Internet voting and undetectable electoral fraud. IEEE Security & Privacy, 17(4): 62-70. https://doi.org/10.1109/MSEC.2019.2915398

[9] Specter, M.A., Koppel, J., Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in US Federal Elections. In 29th USENIX Security Symposium (USENIX Security 20), pp. 1535-1553.

[10] Lewis, K.M., Rice, T.W. (2005). Voter turnout in undergraduate student government elections. PS: Political Science & Politics, 38(4): 723-729. https://doi.org/10.1017/S1049096505050201

[11] Haines, T., Lewis, S. J., Pereira, O., Teague, V. (2020). How not to prove your election outcome. In 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 644-660. https://doi.org/10.1109/SP40000.2020.00048

[12] Albertson, B., Guiler, K. (2020). Conspiracy theories, election rigging, and support for democratic norms. Research & Politics, 7(3): 2053168020959859. https://doi.org/10.1177/2053168020959859

[13] Shah, S. Kanchwala, Q., Mi, H. (2016). Block Chain Voting System. Economist. https://doi.org/10.12694/scpe.v22i3.1853

[14] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P. (2008). Scantegrity: End-to-end voter-verifiable optical-scan voting. IEEE Security & Privacy, 6(3): 40-46. https://doi.org/10.1109/MSP.2008.70

[15] McCorry, P., Shahandashti, S.F., Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. In Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta,

pp. 357-375. https://doi.org/10.1007/978-3-319-70972-7_20

[16] Pawlak, M., Poniszewska-Marańda, A., Kryvinska, N. (2018). Towards the intelligent agents for blockchain e-voting system. Procedia Computer Science, 141: 239-246. https://doi.org/10.1016/j.procs.2018.10.177

[17] Fusco, F., Lunesu, M.I., Pani, F.E., Pinna, A. (2018). Crypto-voting, a Blockchain based e-Voting System. In Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018), pp. 221-225. https://doi.org/10.5220/0006962102230227

[18] Park, S., Specter, M., Narula, N., Rivest, R.L. (2021). Going from bad to worse: from internet voting to blockchain voting. Journal of Cybersecurity, 7(1): 1-15. https://doi.org/10.1093/cybsec/tyaa025

[19] Khan, K.M., Arshad, J., Khan, M.M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1): 53-62. https://doi.org/10.4018/IJEGR.2018010103

[20] Adiputra, C.K., Hjort, R., Sato, H. (2018). A proposal of blockchain-based electronic voting system. In 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 22-27. https://doi.org/10.1109/WorldS4.2018.8611593