SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

A WEB-BASED SCHEMA FOR E-VOTING BASED ON BLOCKCHAIN AS A SERVICE

Jatin Choudhary[1], Deval Patil[2], Vivek Tiwari[3], Arif Sayed[4]
[1]*K. C. College of Engineering Kopri, Thane(E), Mumbai*
[2]*K. C. College of Engineering Kopri, Thane(E), Mumbai*
[3]*K. C. College of Engineering Kopri, Thane(E), Mumbai*
[4]*K. C. College of Engineering Kopri, Thane(E), Mumbai*

ABSTRACT
Blockchain technology is most effective in situations that present opportunities for fraud. In a public or private activity like voting or polling, it assures the integrity of the process as well as the immutability of the data vis-a- vis the poll/vote. Anonymity and privacy for the voter can also be integrated into the overall scheme. This paper explores the potential of blockchain-based e-voting systems in various domains, focusing on their benefits and implementation challenges.
KEYWORDS: *Blockchain technology, e-Voting, Blockchain as a Service (BaaS), Decentralized application (dApp), Smart contracts, Consensus mechanism, Cloud- based hybrid blockchain, Homomorphic encryption, Zero-knowledge proofs, Proof of Authority (PoA), Edge computing.*

INTRODUCTION

The current environment features a scenario where netizens are periodically faced with multiple choices vis-a-vis their affiliation. This could be on any of the following platforms:

- **National, state & local civil body elections:** National and local government election commissions can utilize blockchain technology to ensure the integrity, transparency, and security of voting processes during elections.
- **Non-Governmental Organizations (NGOs):** NGOs conducting internal elections or polls can use blockchain to ensure fairness, transparency, and accountability in the voting process among their members or stakeholders.
  Corporations: Large corporations can implement blockchain-based voting systems for shareholder meetings or board elections, providing shareholders with a secure and transparent way to cast their votes remotely.
- **Trade Unions:** Labor unions can adopt blockchain technology for conducting member voting on collective bargaining agreements, leadership elections, and other important decisions, ensuring democratic processes and transparency.
- **Political Parties:** Political parties can implement blockchain-based voting systems for selecting candidates, conducting primaries, or making internal policy decisions, ensuring transparency and fairness in the party's decision-making process.
- **Online Platforms and Social Networks:** Online platforms and social networks can integrate blockchain technology into their voting features to prevent manipulation of polls or surveys and enhance the credibility of user- generated content.
- **Public Initiativesand Referendums:** Governments or organizations conducting public initiatives, referendums, or opinion polls can leverage blockchain technology to ensure the integrity and security of the voting process, increasing public trust and participation.

The above is made possible due to

- Faster processing and transmission of data; and increasingly efficient networking enable near real-time communication for vast amounts of data.
- Enhanced data storage at steadily decreasing cost.
- High-speed data tools for transactional as well as analytic processing.
- The provision of blockchain technology renders the entire polling process immutable, secure, transparent, and free from third-party interference.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

We posit that a blockchain-based e-voting framework that could be based on demand as a service is viable. It can be used to accrue the advantages of blockchain. We further posit that offering such a scheme on the cloud via the web as a decentralized application will render it more pervasive; as well as enhance its amenability to scale.

Research Aims

The research focuses on exploring the viability of implementing a blockchain-based e-voting mechanism in public scenarios. It aims to investigate the practicality and effectiveness of such a system in enhancing the security, transparency, and accessibility of voting processes. Additionally, the study aims to identify the specific real-life domains, such as national elections, organizational polls, or community decisions, where blockchain-based e-voting can offer significant value. Furthermore, the research seeks to determine the key features and requirements that such a system must possess to ensure its successful implementation and adoption in various voting scenarios.

Review of Literature

Alvi et al [1] developed a scheme for a secure, decentralized methodology to conduct digital voting based on blockchain. The various entities involved in the process and the procedure involved therein were implemented through smart contracts.

Jayakumari et al [2] outlined an E-voting system using cloud-based hybrid blockchain technology. They deployed the Byzantine fault tolerance (PBFT) consensus mechanism and smart contracts. The blockchain assures the integrity of the votes cast.

Hjálmarsson et al. [3] present a blockchain- based e-voting system, exploring the application of blockchain technology in voting systems and discussing its potential benefits.

Monrat et al. [4] provide a comprehensive survey of blockchain technology from various perspectives, including its applications, challenges, and opportunities. It offers insights into the current state of blockchain research and its potential future directions.

Hanifatunnisa and Rahardjo [5] discuss the design of a blockchain-based e-voting recording system. It outlines the architecture and implementation details of the system.

Panja and Roy [6] present a secure end-to- end verifiable e-voting system using blockchain and cloud server technology. It highlights the security features and implementation aspects of the proposed system.

Huang et al. [7] provide an overview of how blockchain technology is applied in voting systems. It covers topics like system architecture, security features, consensus mechanisms, and real-world examples.

George, L., & Kizhakkethottam, J. J. [8] present a comparative study of zero- knowledge proofs and homomorphic encryption in ensuring data privacy in blockchain applications. It discusses the advantages and limitations of both techniques and their effectiveness in guaranteeing privacy in blockchain systems.

Damgård, I., Fazio, N., & Nicolosi, A. [9] introduces a method for achieving non- interactive zero-knowledge proofs from homomorphic encryption. It explores the theoretical foundations of zero-knowledge proofs and their connection to homomorphic encryption schemes.

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. [10] provide a technology review of blockchain-based e- voting systems. It discusses the architectures, applications, and challenges associated with implementing blockchain technology in e- voting systems.

Song, J., Zhang, P., Alkubati, M., Bao, Y., & Yu, G. [11] reviews research advances on blockchain-as-a-service (BaaS), focusing on architectures, applications, and challenges. It discusses the role of BaaS in enabling the deployment and management of blockchain solutions in various domains.

Jafar, U., Aziz, M. J. A., & Shukur, Z. [12] present a review of blockchain for electronic voting systems, discussing the current state of the art, challenges, and open research issues in implementing blockchain technology for e-voting.

Yang, W., et al. [13] present a survey on blockchain-based internet service architecture, discussing the requirements, challenges, trends, and future directions. It explores the integration of blockchain technology into internet services and applications.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

Nguyen, D. C., et al. [14] discusses the integration of blockchain and the cloud of things (CoT), focusing on architecture, applications, and challenges. It explores the potential of combining blockchain and CoT technologies to enable secure and decentralized IoT systems.

Gai, K., et al. [15] present3 a survey on the integration of blockchain and cloud computing, discussing architectures, applications, and challenges. It explores how blockchain technology can enhance the security, efficiency, and scalability of cloud- based systems.

Zhu, L., et al. [16] present a study on controllable and trustworthy blockchain- based cloud data management. It discusses the architecture, applications, and challenges of utilizing blockchain technology for managing data in cloud environments, focusing on control and trustworthiness aspects.

Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. [17] provides an overview of blockchain consensus algorithms, covering various approaches used to achieve agreement among network participants in a decentralized system. It analyzes the characteristics, advantages, and challenges associated with different consensus mechanisms in blockchain networks.

Envisioned System Architecture

The envisioned architecture comprises a Security Hub, Verification Node, Web Portal, Election Authority, Voter, Edge, Cloud Servers, and Blockchain. Security Hub with the help of Verification Node, is responsible for registration and authentication of the Voter [2]. The Election Authority interacts with the Security Hub to oversee the election process. Security Hub interacts directly with the Cloud Server as it sends the encrypted votes for their validation as a transaction and eventual storage in the Blockchain. Processes regarding counting votes and displaying results are done at the Edge Server to tackle concerns regarding performance and scalability. [2][11][13][15][16]

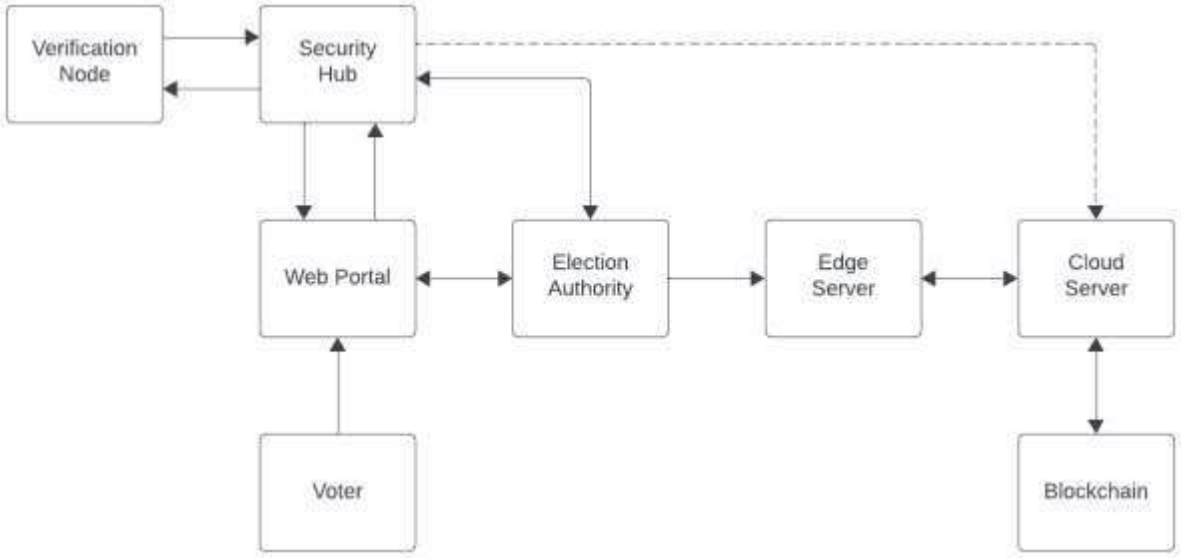


Fig. 1 – Envisioned System Architecture

The architecture is to be developed in phases. For the first phase, we have implemented a scheme for online voting based on blockchain. It will be migrated to the cloud after testing its efficacy in various live environments.

Architecture of Proposed System

The architecture of the proposed methodology is shown in the following figure, Fig. 2, based on blockchain technology.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

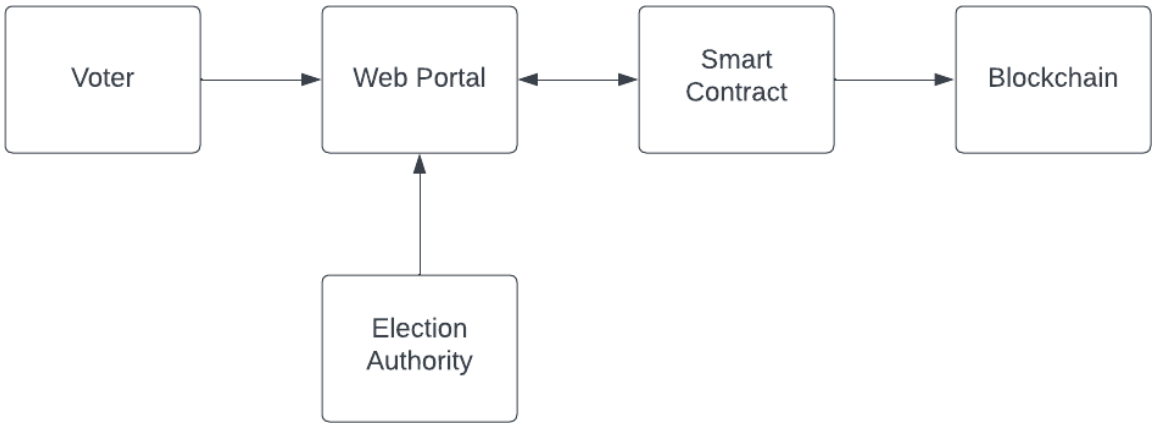


Fig. 2 – Proposed System Architecture

The proposed system architecture consists of Voter, Web Portal, Smart Contract, Election Authority and the Blockchain. Voters interact with the system through a user-friendly Web Portal, casting their votes securely. Behind

the scenes, a Smart Contract deployed on the blockchain manages the recording of votes. Each vote is securely stored on the blockchain, creating an immutable and transparent ledger of the electoral process. The Election Authority administers the process through the Web Portal, overseeing tasks such as voter registration and result declaration.

To understand the system better, the following diagram, Fig. 3, depicts how things are working behind the scenes:

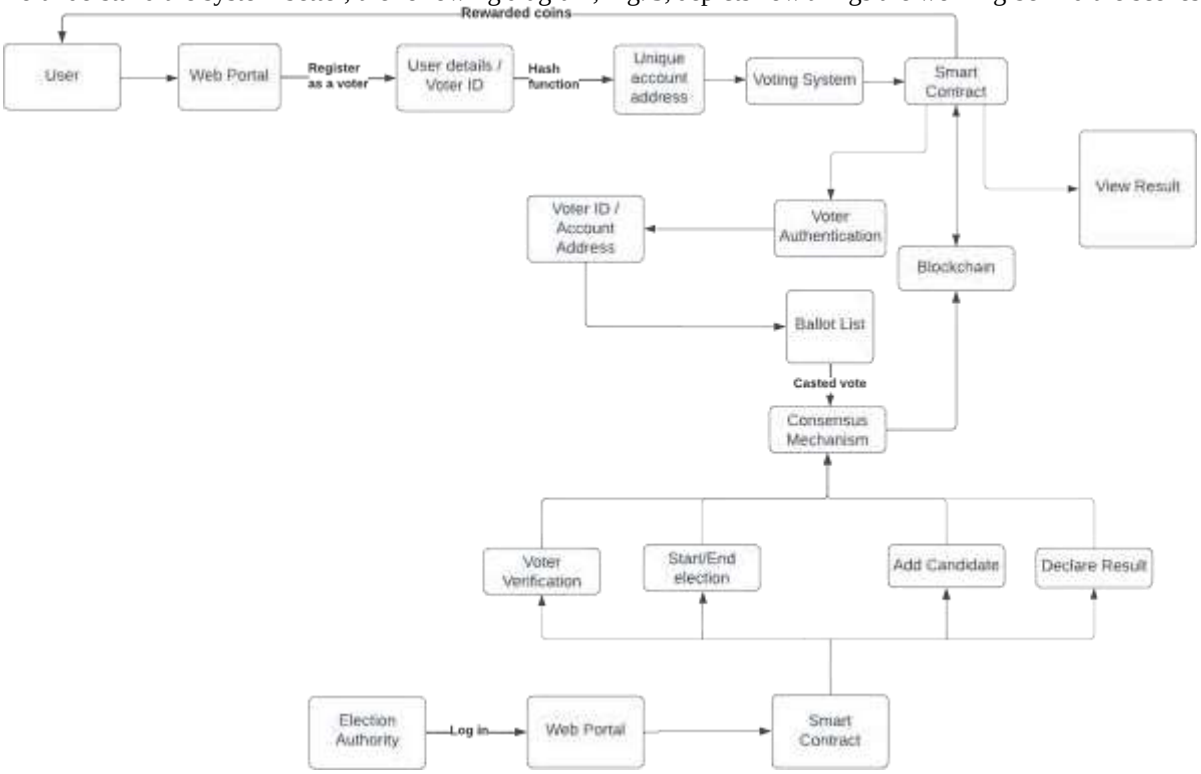


Fig. 3 – Detailed System Architecture

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

Voting Process

When a voter casts their vote, the vote is encrypted with the voter id, and the candidate's public key they are voting to, and is sent to the validators in the consensus mechanism as a transaction where they validate it and store it in the blockchain.
The votes of the candidate are counted and tallied through the algorithmic operations that the Homomorphic Encryption technique allows us to perform. Homomorphic encryption is a form of encryption that allows certain mathematical operations to be performed on encrypted data without decrypting it. One can perform computations on encrypted data and obtain the same result as if the operations were performed on the unencrypted data. [8][9]
The total votes are then displayed using Zero- Knowledge Proof cryptographic protocol at the time of the result declaration.

Zero-knowledge proofs are cryptographic protocols that allow one party (the prover) to prove to another party (the verifier) that they know a certain piece of information without revealing any additional information beyond the validity of the statement. [8][9]

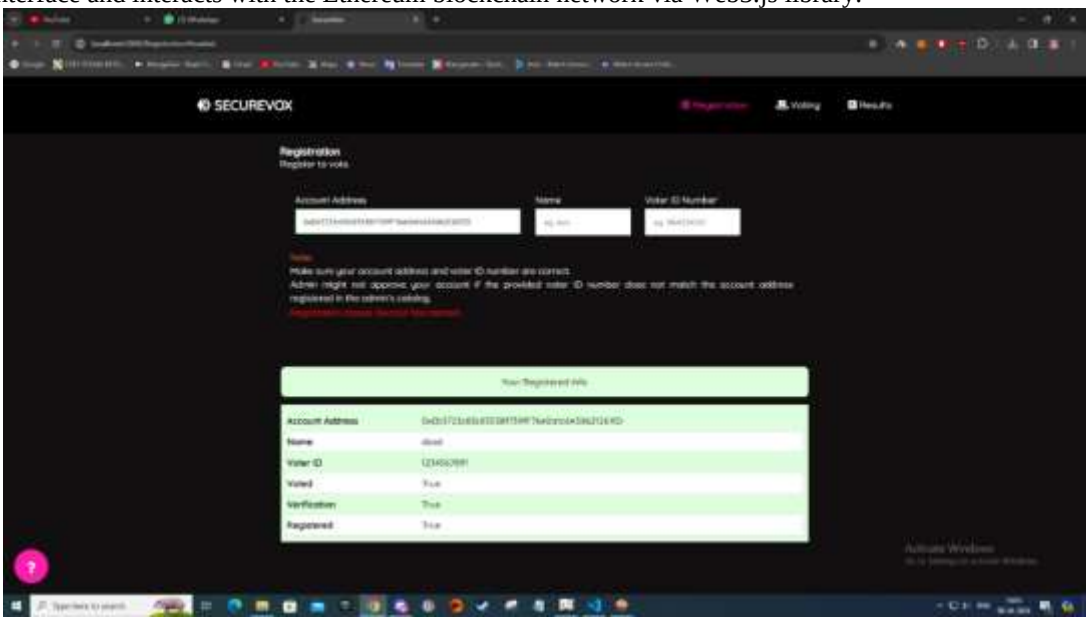
Consensus Mechanism

In the proposed system, we plan to integrate the Proof of Authority (PoA) consensus mechanism to achieve high performance, efficiency, and governance control.
PoA consensus mechanism ensures that only trusted entities, such as verified institutions or individuals whitelisted by the election authority, have the authority to validate and confirm voting transactions. This enhances the security and reliability of the electoral process, as the consensus process is controlled by known and reputable validators. [10][17]
By integrating PoA into our voting system, we can achieve efficient block confirmation times, high transaction throughput, and robust governance controls, ensuring the integrity and transparency of the online voting process.

Implementation Instance

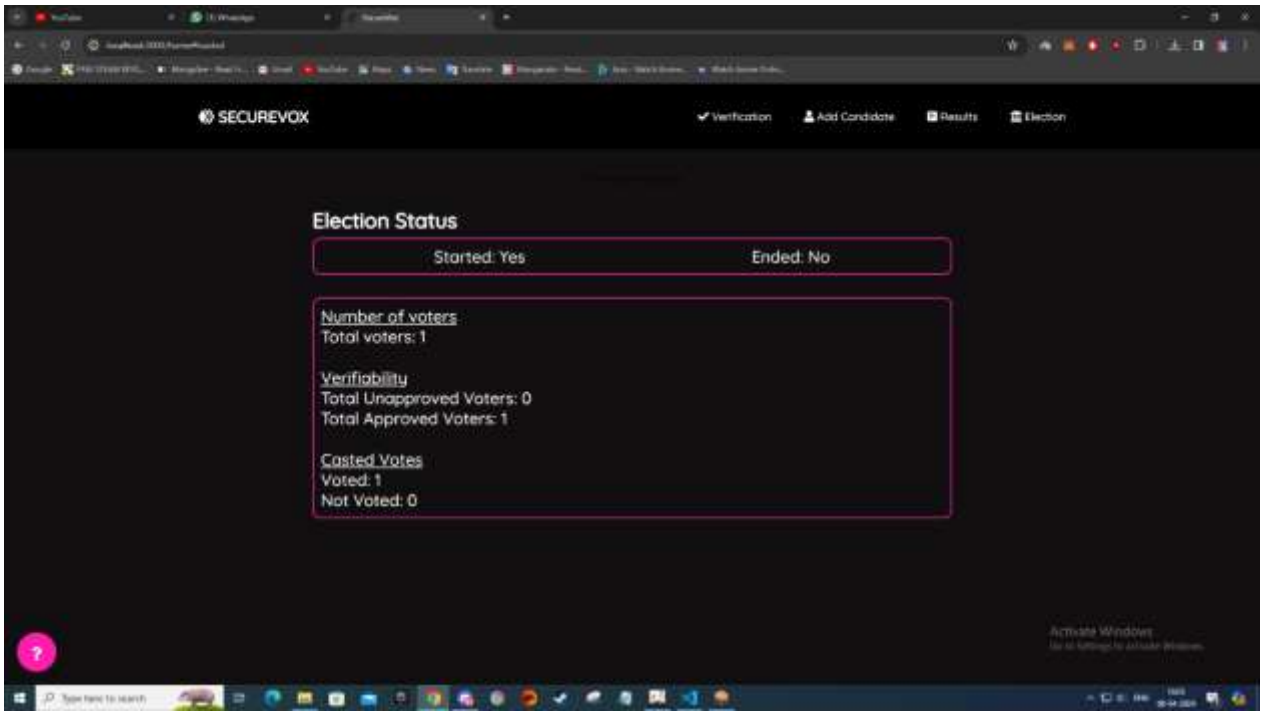
Our implementation instance includes the following components:

1. **Truffle:** Truffle is used as our development framework for building, testing, and deploying smart contracts. It provides a suite of tools for smart contract development, including compilation, testing, and deployment capabilities.
2. **Solidity:** Solidity is the programming language used to write our smart contracts. It is specifically designed for writing Ethereum smart contracts and allows us to define the behavior of our decentralized voting system.
3. **Ganache:** Ganache is used as our local blockchain network for development and testing purposes. It provides a simulated Ethereum blockchain environment where we can deploy and interact with our smart contracts without incurring actual gas costs.
4. **Node Server:** A Node.js server is utilized for backend operations and integration with external components. It communicates with the frontend interface and interacts with the Ethereum blockchain network via Web3.js library.

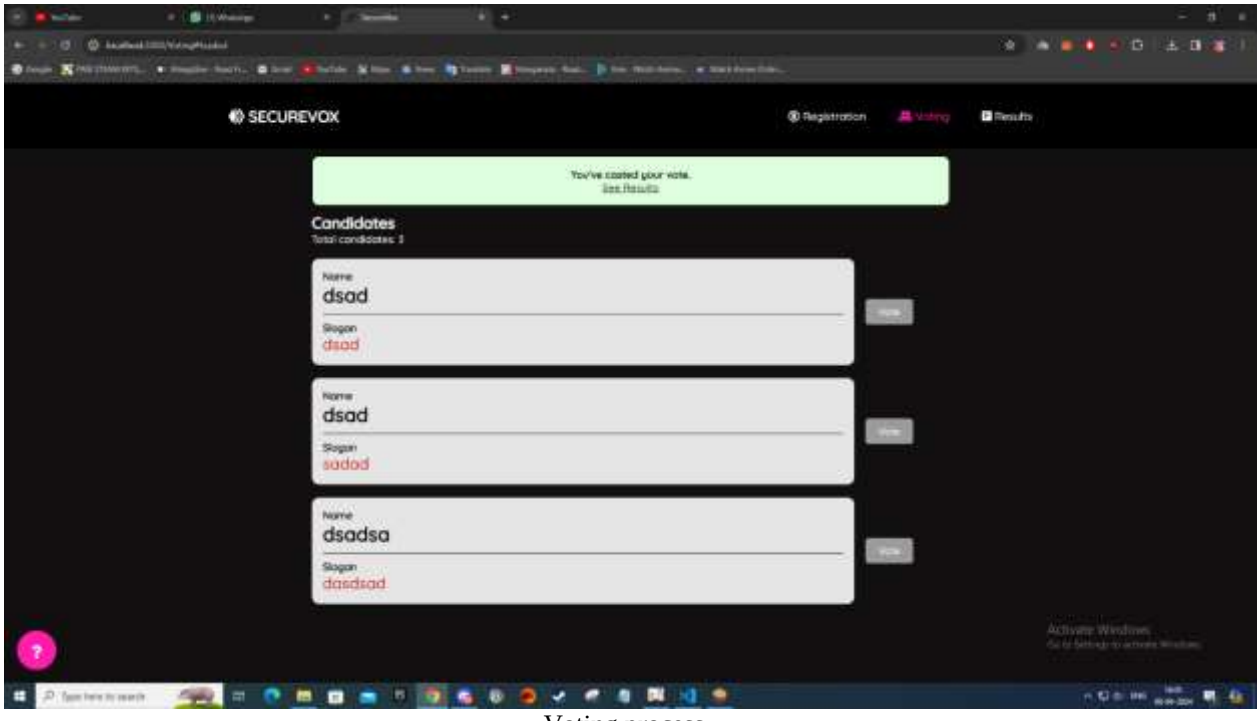


Voter Registration

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

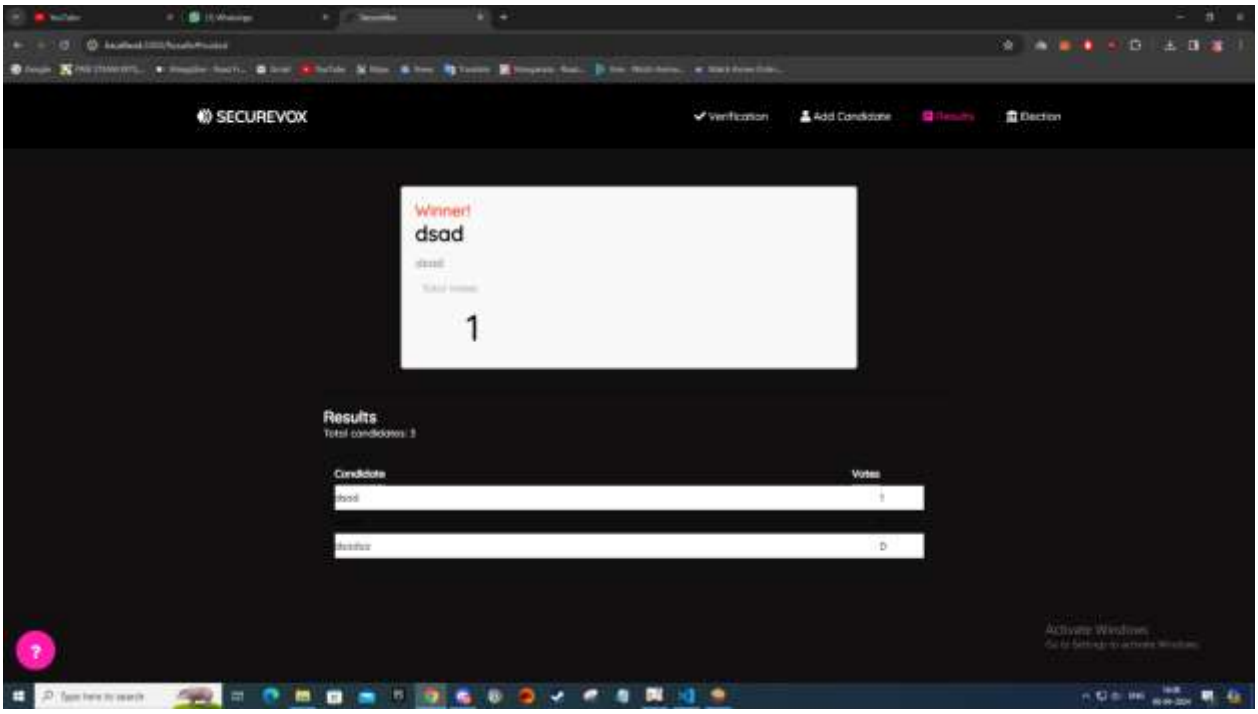


Election Status



Voting process

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal



Election Result

Result Analysis

TC Sr.no	Description	Expected output	Actual output	Pass/Fail
1.	Voter registration	Successful registration of voters	Voter gets registered into the system, waits for being verified by admin	Pass
2.	Voter authentication	Voter verification	The admin verifies voter details/credentials and authenticates them to participate in elections	Pass
3.	Candidate registration	Registration of candidates contesting for elections	Admin adds the candidates name who are about to contest in elections in the ballot	Pass
4.	Voting	Voters select and vote for candidates	The voters use a coin assigned to them so they can vote for a candidate.	Pass
5.	End elections	End of election	The admin ends the election and can view the results and declare them	Pass

Features

Decentralized and Transparent: Leveraging blockchain technology ensures decentralization and transparency, eliminating the need for intermediaries and providing a tamper-resistant record of the voting process.

Secure Encryption: Votes are encrypted using public-private key pairs generated by the Crypto Server, ensuring voter anonymity and privacy.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

Smart Contract Automation: Smart contracts automate various aspects of the election process, including voter registration, candidate registration, vote casting, and result declaration, reducing manual intervention and enhancing efficiency.

Voter Authentication: Authentication mechanisms ensure that only verified voters can participate in the voting process, enhancing security and preventing fraudulent activities.

Scope for further research

Scalability: Investigate techniques to enhance the scalability of blockchain-based voting systems to accommodate a larger number of voters and transactions without compromising performance.

Voter Accessibility: Explore methods to make blockchain-based voting systems more accessible to voters with disabilities or limited access to technology, ensuring inclusivity and equal participation.

Vulnerability Assessment: Conduct thorough vulnerability assessments and security audits of blockchain-based voting systems to identify and mitigate potential security threats and vulnerabilities.

Conclusion

Human society is on the cusp of the Fifth Industrial Revolution. This entails that the layman should feel more comfortable with machines and automated processes.

REFERENCES

1. *Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed, "DVTChain: A blockchain- based decentralized mechanism to ensure the security of digital voting system voting system" Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, October 2022, Pages 6855-6871*
2. *Beulah Jayakumari, S Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya, Malathy Jawahar, "E-voting system using cloud-based hybrid blockchain technology" Journal of Safety Science and Resilience, Volume 5, Issue 1, March 2024, Pages 102-109*
3. *Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e- voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.*
4. *A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi:10.1109/ACCESS.2019.2936094.*
5. *R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA),Lombok, Indonesia, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.*
6. *Somnath Panja, Bimal Roy, A secure end-to-end verifiable e-voting system using blockchain and cloud server, Journal of Information Security and Applications, Volume 59, 2021,102815,ISSN 2214-2126,https://doi.org/10.1016/j.jisa.2021.10 2815. (https://www.sciencedirect.com/scie nce/article/pii/S2214212621000557)*
7. *Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo,K. K. R. (2021). The application of the blockchain technology in voting systems: A review. ACM Computing Surveys (CSUR), 54(3), 1-28.*
8. *[Liz George and Jubilant J. Kizhakkethottam (2021); A COMPARATIVE STUDY OF ZERO KNOWLEDGE PROOF AND HOMOMORPHIC ENCRYPTION IN GUARANTEEING DATA PRIVACY IN BLOCKCHAIN APPLICATIONS Int. J. of Adv. Res. 9 (Feb). 359-361] (ISSN 2320-5407).*
9. *Damgård, I., Fazio, N., Nicolosi, A. (2006).Non-interactiveZero- Knowledge fromHomomorphic Encryption. In: Halevi, S., Rabin, T. (eds) Theory of Cryptography. TCC 2006. Lecture Notes in Computer Science, vol 3876. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11681878_3*
10. *Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain- Based E-Voting Systems: A Technology Review. Electronics. 2024;13(1):17. https://doi.org/10.3390/electronics13 010017*
11. *Song, J., Zhang, P., Alkubati, M., Bao, Y., & Yu, G. (2022). Research advances on blockchain-as-a-service:Architectures, applications and challenges. Digital Communications and Networks, 8(4), 466-475.*
12. *Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System – Review and Open Research Challenges. Sensors. 2021; 21(17):5874.https://doi.org/10.3390/s21175874*
13. *Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A survey on blockchain- based internet service architecture: requirements, challenges, trends, and future. IEEE access, 7, 75845-75872.*
14. *Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications andchallenges.IEEE Communications surveys & tutorials, 22(4), 2521-2549.*

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

15. *Gai, K., Guo, J., Zhu, L., & Yu, S.(2020). Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials, 22(3), 2009-2030.*
16. *Zhu, L., Wu, Y., Gai, K., & Choo, K.R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527-535.*
17. *Ferdous, M. S., Chowdhury, M. J. M.,Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. arXivpreprint arXiv:2001.07091.*