Blockchain-based decentralized voting system with SHA-256 algorithm and facial recognition

BJD Kalyani[1], Jaya Krishna Modadugu[2], Sarabu Neelima[3]
[1]Department of Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, India
[2]Software Engineer III, Prosper Marketplace Inc, San Francisco, United States
[3]Department of Computer Science and Engineering, Priyadarshni Institute of Science and Technology for Women, Khammam, India

Article Info

Article history:

Received Apr 16, 2024
Revised Apr 26, 2025
Accepted Jun 10, 2025

Keywords:

Blockchain technology
Digital identity verification
Electronic voting system
Ethereum
SHA-256

ABSTRACT

Blockchain technology has completely changed the way data is stored and transactions are verified. It provides a dependable, transparent, and safe medium for communication and transaction validation. In order to solve the drawbacks of conventional electronic voting systems, the goal of this research project is to design a decentralized voting system based on blockchain technology. The suggested method offers an immutable and safe way to record and validate votes by utilizing the security and transparency capabilities of blockchain technology. The suggested approach provides an immutable and safe way to record and validate votes by utilizing the security and transparency capabilities of blockchain technology. This paper aims to provide a comprehensive process for digital identity authentication, create a voter interface that is compatible with Ethereum wallets, and apply smart contracts on the Ethereum network to speed up voter registration, ballot preparation, voting, and result tabulation. Additionally, this paper proposes to build up a multi-factor authentication system for election managers and validators to offer them safe and approved power over the voting process. By carefully examining the existing methods, this research highlights the flaws and weaknesses of traditional electronic voting systems and stresses the need for more trustworthy and secure voting technology. The proposed blockchain-based voting system offers an innovative solution to problems with voter fraud and election manipulation because of its irreversible blockchain record, which gives a high degree of transparency and integrity.

Corresponding Author:

BJD Kalyani
Department of Computer Science and Engineering, Institute of Aeronautical Engineering
Telangana, Hyderabad, India
Email: kjd_kalyani@yahoo.co.in

1. INTRODUCTION

The techniques for data storage and transaction verification have undergone a fundamental transformation as a result of the use of blockchain technology [1]. Blockchains, or distributed digital ledgers [2], are a revolutionary technology that enables network participants to confirm transactions and communicate in a secure, immutable, and transparent manner without the need for intermediaries [3]. Despite its apparent simplicity, the core concept of blockchain technology is the creation of data blocks linked together in a chain [4]. By adding a hash a unique code made from the contents of the block and connecting to the block that came before it, each block creates an immutable chain [5]. A block cannot be removed or changed from the blockchain after it has been posted without the network's members' approval [6]. Data stored on the blockchain is certain to remain transparent and untouched by tampering due to its immutability.

Blockchain-based decentralized voting systems might have a big influence on elections. Because these technologies offer a reliable and secure way to record and validate votes [7], they have the potential to boost voter turnout and restore faith in the democratic process. Decentralized voting systems can also significantly reduce the costs and administrative strains associated with traditional voting procedures [8], enhancing election accessibility and inclusivity [9].

The security and transparency of blockchain technology have led to its widespread application in a number of areas, including as supply chain management, healthcare, and finance [10]. Regarding voting systems, these characteristics are highly advantageous. Votes in decentralized voting systems are recorded on an irreversible blockchain ledger, offering a high degree of transparency and integrity. This effectively resolves worries about election manipulation and fraud [11].

In view of this, the purpose of this research project is to use blockchain technology's revolutionary potential to construct a decentralized voting system that would solve the problems with the present electronic voting systems. Using cutting-edge technology like facial recognition and the SHA-256 algorithm [12], the proposed solution enhances security and authentication processes.

The programme aims to achieve many objectives. Its primary goal is to provide a comprehensive process for digital identity verification [13] that uses public-private key pairs and digital signatures to safely authenticate and authorize voters [14]. The project's second goal is to create a user-friendly interface that works with Ethereum wallets so that voters may safely use their Ethereum accounts to cast ballots via the electronic voting system [15].

In addition, a robust multi-factor authentication system will be put in place to provide secure access to and management of the e-voting smart contracts by validators and election administrators, enabling voting process monitoring [16]. This multi-factor authentication system will be an essential line of defence against illegal access and vote-process manipulation. In addition, the system will provide real-time event recording and monitoring capabilities to provide complete control over the voting process and an audit trail. By enabling stakeholders to watch over and verify each vote step, this innovation will increase accountability and transparency [17].

2. RESEARCH METHOD

2.1. Literature review

Henry *et al.* [18] focused-on voting subject to the primary database's high-security password being verified. Voters have the ability to determine if a certain party or candidate has profited from vote rigging. Manual vote counting, which maintains voter data and guarantees the integrity of the voting process, is a secure and transparent method of verifying voter accuracy. Kleinaki *et al.* [19] are concentrates on utilization of Aadhar card database for targeted identification and fingerprint technology for verification in order to establish a safe electronic voting system. The primary objective is to enable secure online voting during elections through the use of finger vein identification technology. This will initiate an electronic poll reset and facilitate voter casting. The technique uses fingerprint technology and the Aadhar card database to improve voting process security and accuracy. This guarantees accurate voting records and voter identity verification. Finger vein detection technology not only provides a trustworthy way to identify voters, but it also fixes problems with data integrity and authentication in the election process and enhances the security and efficacy of electronic voting.

Kaur *et al.* [20] are describing a data security technique that leverages advanced hashing algorithms. The paper proposes block-creation and block sealing as ways to enhance the applicability of blockchain technology to the specific requirements of the polling approach. According to block sealing theory, the blockchain system may be made more flexible by tailoring it to the needs and guidelines of the polling procedure. By employing this technique, election- related blockchain technology may be optimized while simultaneously enhancing data security and consistency. By employing this technique, election-related blockchain technology may be optimized while simultaneously enhancing data security and consistency. The focus of the study on hashing algorithms and block sealing demonstrates a commitment to enhancing the flexibility and robustness of blockchain systems for use in critical applications. Pirtle and Ehrenfeld [21] offers a thorough security analysis of an actual Indian electronic voting machine (EVM) system. The analysis reveals a number of vulnerabilities in the EVM, including the possibility of manipulation through machine state changes, pre-manufacturing software modifications, and swapping out comparable units or CPUs, all of which might risk voter privacy. These previously noted drawbacks are addressed by the suggested voting technique, which does away with the substantial hardware needs of conventional EVMs. The suggested approach seeks to build a more trustworthy and secure voting mechanism that protects against the identified shortcomings and preserves the integrity and secrecy by addressing these concerns and emphasizing a hardware-independent voting procedure.

A comprehensive analysis of a blockchain-based voting system in lecture notes on data engineering and communications technologies. Their research demonstrates how the verifiability and openness of the political process may be enhanced by an auditable blockchain voting system. The authors present how the shortcomings of traditional voting methods may be addressed by using the technological details and architectural elements of the system. Our grasp of how blockchain technology may reinforce and enhance voting methods has been improved as a result of this work. Their study sheds light on the potential benefits of blockchain- based voting systems and provides useful details regarding current technological advancements.

2.2. Existing framework

Voters are required by the current system to physically visit a polling location and utilize paper ballots. These votes are then carefully tallied and documented. Additionally, several countries have adopted electronic voting systems that allow people to use voting machines or the internet to cast their ballots. However, security flaws and other vulnerabilities have drawn criticism for electronic voting techniques. Due to the traditional electronic voting systems' susceptibility to different cyberthreats, voter privacy and election integrity are significantly in risk. One of these weaknesses might be hacking, which could result in the tampering of election results and unapproved access to voter personal information. The interconnectedness of computer systems increases the risk of data breaches and illegal access. Moreover, the absence of strong security protocols in these systems renders them vulnerable to exploitation by malevolent entities.to being used by unscrupulous parties. These weaknesses put the credibility of the democratic process in jeopardy by compromising the confidentiality of voters' decisions and casting doubt on the accuracy of the outcomes. To protect electronic voting systems' security and privacy, preserve public safety, and preserve democracy, these weaknesses must be fixed as in Figure 1.

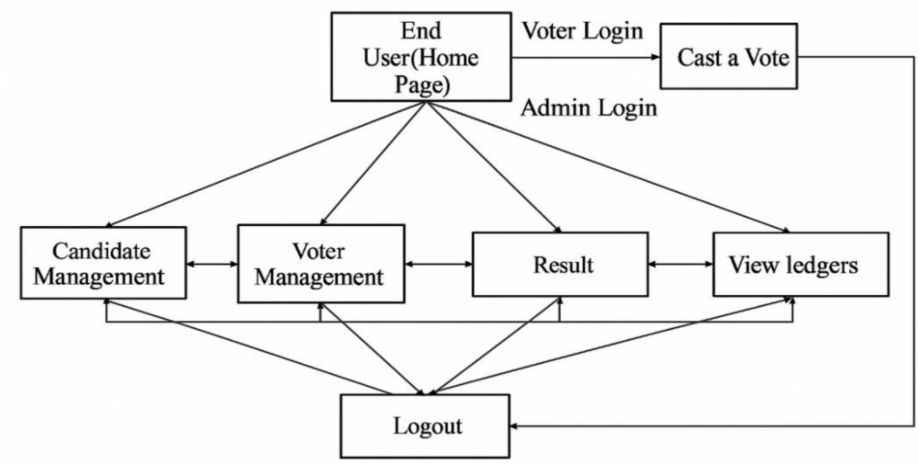


Figure 1. Dataflow diagram of existing framework

Due to inherent problems with data integrity, auditability, and the possibility of anomalies or mistakes throughout the voting process, conventional electronic voting systems are frequently seen as unreliable and untrustworthy. The integrity of the election results is questioned in light of the weak procedures in place to guarantee the privacy and accuracy of vote data. Furthermore, the public's confidence in the democratic process is weakened by the systems' restricted auditability, which makes it more difficult to confirm the veracity of the results. More dependable and secure voting technology is required because of these systems' susceptibility to anomalies and mistakes during voting processes, which casts doubt on the system's overall reliability.

2.3. Method

The security, transparency, and integrity of the voting mechanisms are now lacking, which is the root of the issue. Conventional voting methods depend on face-to-face meetings and paper ballots, yet worries have been expressed regarding possible security flaws in electronic voting systems that might endanger voter privacy and the integrity of the election process. There are major risks associated with vulnerabilities including result manipulation, hacking, and unauthorized access to voter data. Furthermore, the perceived volatility and lack of auditability of traditional electronic voting methods erode public faith in the democratic process. These issues demonstrate how important it is to have voting technology that is more dependable, safe, and trustworthy in order to preserve fair and transparent elections. These problems need to be fixed in order to preserve election integrity, safeguard voter privacy, and maintain the legitimacy of the democratic process.

The blockchain-based voting system's suggested technique is a ground-breaking development in electoral systems. This novel strategy transforms elections by utilizing the built-in security and transparency of blockchain technology. Using a decentralized digital ledger, the system eliminates the need for middlemen by ensuring safe and irreversible communication and transaction verification. Voting is facilitated via a front-end interface, while back-end software processes votes. The Ethereum blockchain is used for safe record-keeping. Improving the transparency and integrity of election processes is a major step forward with the introduction of a blockchain-based voting system as in Figure 2.

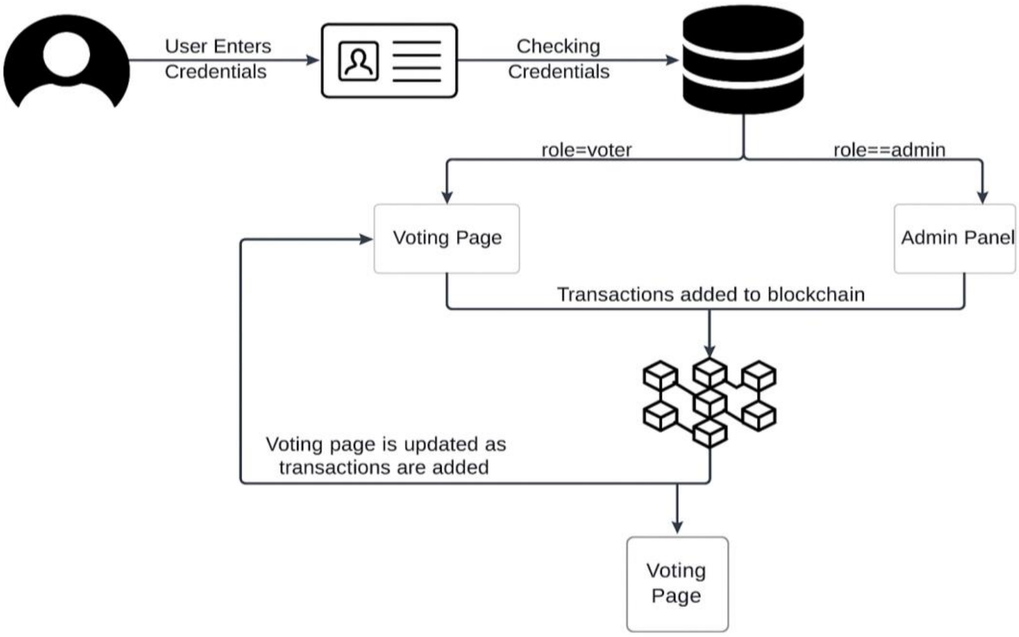


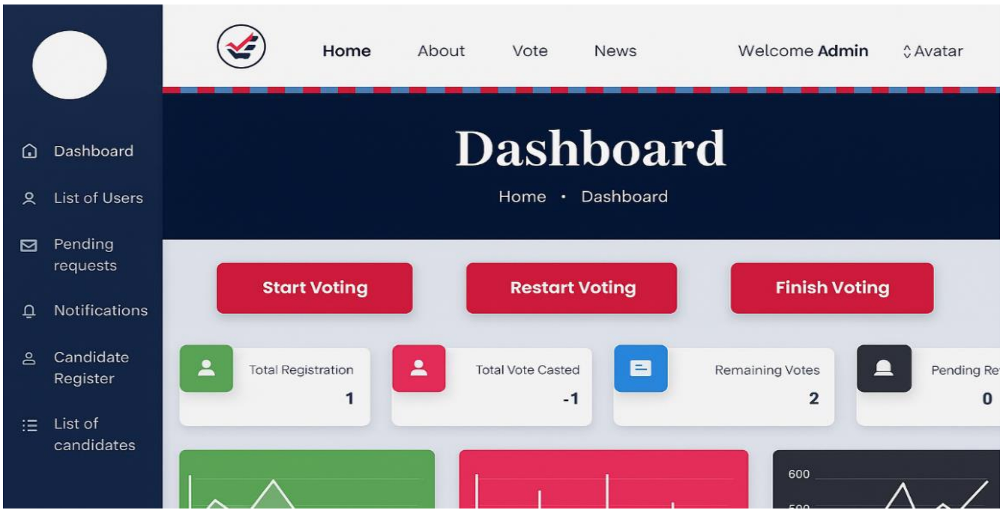
Figure 2. Proposed system architecture

There will be a strong voter validation mechanism in place to guarantee the validity of the voting process. Voter IDs and facial recognition will be used for two-factor authentication for eligible voters, boosting security and thwarting unwanted access. Additionally, voter data and transactions on the blockchain will be secured by cryptographic techniques like the SHA-256 algorithm and digital signatures, strengthening the system against any security attacks. The system will be further strengthened against vulnerabilities with regular security audits and testing. Smart contracts deployed on the blockchain will oversee the election process, guaranteeing transparency and immutability at every stage, including voter registration, candidate nomination, ballot casting, vote counting, and result announcement. Voters and the system will be able to engage restlessly thanks to the encoding of business logic into smart contracts, which will improve voting process security and transparency. To promote smooth voter involvement, the front-end interface will be created with an easy-to-use and intuitive layout. Through the use of the previously indicated strategy, the blockchain-based voting system seeks to further democratic processes by offering a safe, transparent, and effective platform for holding elections.

3. RESULTS AND DISCUSSION

In several essential components and processes need to be implemented in order for the blockchain-based voting system to be safe and effective. Smart contracts will be used to encrypt the business logic governing voter registration, candidate nomination, and vote casting. The system's secure and decentralized design will be based on the Ethereum blockchain. Through the use of thrustless interactions, these smart contracts will increase voting process security and transparency. A comprehensive voter validation system, which combines voter ID with facial recognition technology, will confirm the eligibility of voters. This two-factor authentication method, which limits the number of votes to those who are allowed, will improve election security. Furthermore, the SHA-256 algorithm and additional cryptographic approaches will safeguard voter data and transactions on the blockchain, providing an additional layer of protection against any security breaches.

The election system will use blockchain-based smart contracts to enforce deadlines and regulations at every voting stage, guaranteeing the election's immutability and integrity. Transparency and justice will be upheld by this automatic enforcement, which also removes the chance of manipulation or human interference. The system will also undergo routine security testing and audits to find holes, fix them, and strengthen defences against hackers. The goal of proposed system is to facilitate easy voter involvement, a user-friendly layout will be incorporated into the front-end interface design. Voters will be able to register, recommend candidates as in Figure 3, cast votes, and obtain election-related information via an easy-to-use platform. Every voter will have a seamless and dependable voting procedure thanks to the back-end functionality, which will process votes safely and effectively as in Figure 4.



Dashboard

Home • Dashboard

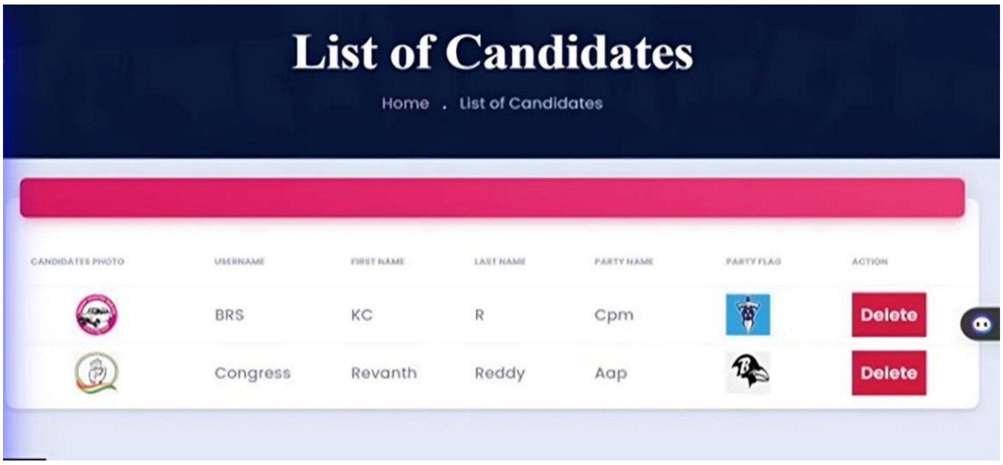
Total Registration 1

Total Vote Casted -1

Remaining Votes 2

Pending Re 0

Figure 3. Admin dashboard



List of Candidates

Home . List of Candidates

CANDIDATES PHOTO	USERNAME	FIRST NAME	LAST NAME	PARTY NAME	PARTY FLAG	ACTION
	BRS	KC	R	Cpm		Delete
	Congress	Revanth	Reddy	Aap		Delete

Figure 4. Candidate details page

The proposed system employed a range of technologies to accomplish our objectives. HTML, CSS, JavaScript, JQuery, and Thymeleaf were utilized in frontend development to create a dynamic and interactive user interface as in Figure 5. For image processing tasks on the backend, we utilized OpenCV, and for some functions, we combined Python and Java. The backend operations were made possible via the spring framework, which comprises spring MVC, spring boot, spring JPA, and hibernate for efficient data administration and interaction. Additionally, spring security was deployed to offer robust security measures. The code made use of MySQL, a database management system that was set up on the Tomcat server. When these technologies worked together, it was simpler to design a comprehensive and secure system that would meet the project's objectives. Additionally, because intelliJ IDEA provided a reliable platform for coding, debugging, and version control, we utilized it as our primary integrated development environment (IDE) for the project's administration and development.

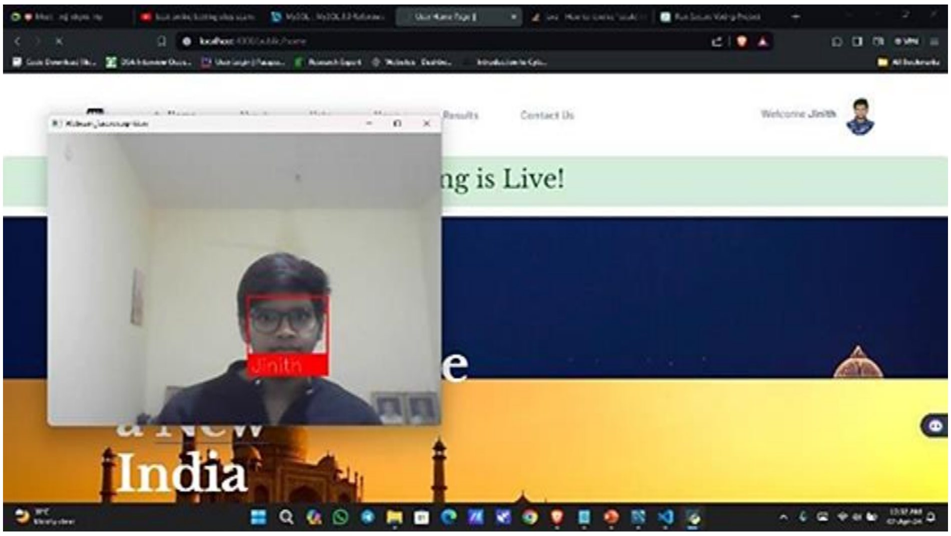
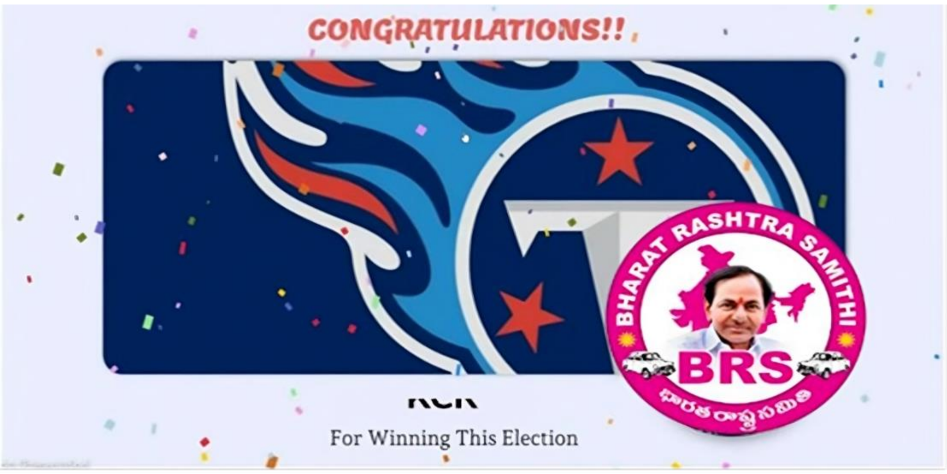


Figure 5. Facial authentication

The blockchain-based voting system will make use of cutting-edge technology, strict security protocols, and automated procedures to provide a safe, transparent, and effective platform for holding elections as in Figure 6.


CONGRATULATIONS!!

KCR

For Winning This Election

Figure 6. Voting result

Figure 7 is used to depict the accuracy % of smart contract execution over a range of time steps, or epochs, that are utilized for model training or contract execution. The accuracy % runs from 0.65 to 0.95 on the vertical axis (y-axis), while the epochs are numbered from 0 to 50 along the horizontal axis (x-axis). The graph is composed of six lines, each of which shows a distinct trend in the execution accuracy of smart contracts over a 50-epoch period. To the right of the graph, in the legend, is a label that corresponds to each color-coded line.

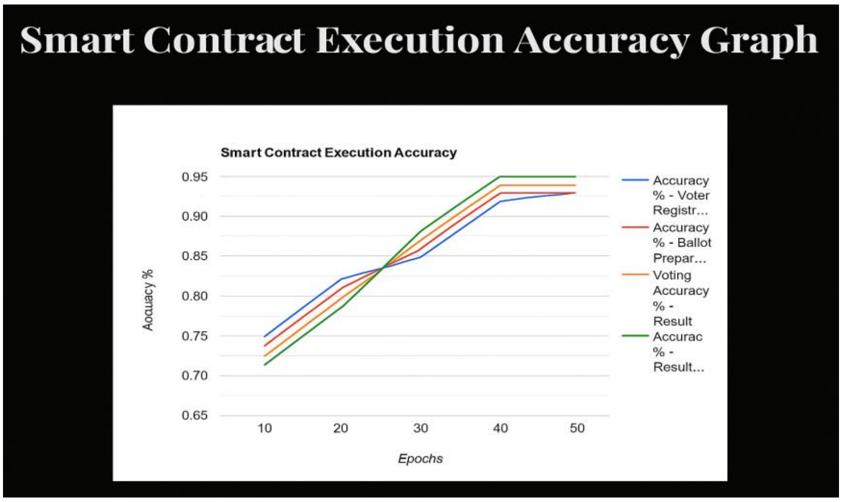


Figure 7. Performance evaluation

4. CONCLUSION

Using the Ethereum blockchain to provide decentralized voting offers an innovative way to hold safe and open elections. This strategy protects the integrity and immutability of cast votes by establishing an impenetrable voting platform through the utilization of blockchain technology. Because the Ethereum blockchain is decentralized, it makes it harder for one party to exert undue influence over the network, which greatly improves voting system security and reliability. The voting process benefits greatly from the openness and auditability that are intrinsic to blockchain technology. On the blockchain, each vote is documented as a block, generating an eternal record that is available to everybody. Voter trust is increased by this transparency, which also allays fears about possible fraud or manipulation and increases faith in the democratic process. Furthermore, there is a great deal of promise in the continuous developments of Ethereum, such as the attempts to increase scalability, interoperability with other cutting-edge technologies, and user interface. The people can vote more easily and clearly if voting procedures are made more user-friendly, which might lead to a rise in voter turnout. Increased scalability will allow the system to process more transactions, allowing for wider election participation without sacrificing effectiveness.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
BJD Kalyani	✓	✓	✓	✓	✓	✓						✓	✓	
Jaya Krishna Moodadugu	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓		
Sarabu Neelima	✓		✓	✓			✓			✓	✓		✓	✓

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available at:

- https://data.telangana.gov.in/dataset/telangana-ulb-elections-2021
- https://data.opencity.in/dataset?organization=election-commission-of-india

REFERENCES

[1] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research*, vol. 14, no. 1, pp. 53–62, Jan. 2018, doi: 10.4018/IJEGR.2018010103.

[2] V. Lenarduzzi, M. I. Lunesu, M. Marchesi, and R. Tonelli, "Blockchain applications for agile methodologies," in *Proceedings of the 19th International Conference on Agile Software Development: Companion*, May 2018, vol. Part F1477, pp. 1–3, doi: 10.1145/3234152.3234155.

[3] A. Pinna, R. Tonelli, M. Orrú, and M. Marchesi, "A petri nets model for blockchain analysis," *Computer Journal*, vol. 61, no. 9, pp. 1374–1388, 2018, doi: 10.1093/comjnl/bxy001.

[4] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-oriented software engineering: Challenges and new directions," *Proceedings - 2017 IEEE/ACM 39th International Conference on Software Engineering Companion, ICSE-C 2017*, pp. 169–171, 2017, doi: 10.1109/ICSE-C.2017.142.

[5] E. Ben-Sasson *et al.*, "Zerocash: decentralized anonymous payments from bitcoin," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 459–474, 2014, doi: 10.1109/SP.2014.36.

[6] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale election based on blockchain," *Procedia Computer Science*, vol. 129, pp. 234–237, 2018, doi: 10.1016/j.procs.2018.03.063.

[7] H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID," in *International Conference on ICT and Knowledge Engineering*, Nov. 2013, pp. 1–4, doi: 10.1109/ICTKE.2013.6756265.

[8] S. Chakraborty, S. Mukherjee, B. Sadhukhan, and K. T. Yasmin, "Biometric voting system using adhar card in India," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 4, pp. 5284–5291, 2016.

[9] V. Kantharaju, M. V. Dhanalakshmi, Nidhi, B. Deepa, and A. Almas, "Secure digital voting system based on blockchain technology - a survey," *International Journal of Scientific Research in Science, Engineering and Technology*, pp. 58–62, May 2022, doi: 10.32628/ijsrset22938.

[10] A. Shah, N. Sodhia, S. Saha, S. Banerjee, and M. Chavan, "Blockchain enabled online-voting system," *ITM Web of Conferences*, vol. 32, p. 03018, Jul. 2020, doi: 10.1051/itmconf/20203203018.

[11] A. S. Yadav, "E-Voting using blockchain technology," *International Journal of Engineering Research and*, vol. V9, no. 07, Jul. 2020, doi: 10.17577/IJERTV9IS070183.

[12] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions," *arXiv*, pp. 1–15, 2017, doi: 10.48550/arXiv.1608.00771.

[13] U. C. Çabuk, T. Şenocak, and E. Demir, "A proposal on initial remote user enrollment for IVR-based voice authentication systems," *International Journal of Advanced Research in Computer and Communication Engineering* (*IJARCCE)*, vol. 6, no. 7, pp. 118–123, 2017, doi: 10.17148/ijarcce.2017.6722.

[14] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10322 LNCS, pp. 357–375, 2017, doi: 10.1007/978-3-319-70972-7_20.

[15] Kostas (Konstantinos) Chalkias, "Demonstrate how zero-knowledge proofs work without using maths," *CordaCon 2017*, 2017, [Online]. Available: https://www.linkedin.com/pulse/demonstrate-how-zero-knowledge-proofs-work-without-using-chalkias/.

[16] N. A. J. Al-Habeeb, N. Goga, H. A. Ali, and S. M. S. Al-Gayar, "A new M-voting system for COVID-19 special situation in Iraq," *2020 8th E-Health and Bioengineering Conference, EHB 2020*, 2020, doi: 10.1109/EHB50910.2020.9280275.

[17] S. Patil, O. Patil, K. Khambait, and A. Bhagwat, "Blockchain technology–fundraising tracking system using blockchain," *International Journal of Novel Research and Development*, vol. 9, no. 3, pp. 186–191, 2024.

[18] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: challenges and directions," *IEEE Security and Privacy*, vol. 16, no. 4, pp. 38–45, 2018, doi: 10.1109/MSP.2018.3111245.

[19] A. S. Kleinaki, P. M. Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A blockchain-based notarization service for biomedical knowledge retrieval," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 288–297, 2018, doi: 10.1016/j.csbj.2018.08.002.

[20] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of Medical Systems*, vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-1007-5.

[21] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: the next generation of medical records?," *Journal of Medical Systems*, vol. 42, no. 9, 2018, doi: 10.1007/s10916-018-1025-3.

BIOGRAPHIES OF AUTHORS

BJD Kalyani working as Associate Professor in the Department of Computer Science and Engineering at Institute of Aeronautical Engineering. Awarded doctorate from Acharya Nagarjuna University, Guntur in the area of Cloud computing. She is having 6 years of industry and 12 years of teaching experience. She guided 8 PG projects and 20 UG projects. She published 15 papers in various national/international conferences and journals. Her research areas of interest are cloud computing, data analytics, business intelligence, software engineering, and database management systems. She is associated with several committees like R&D, discipline, anti ragging and hospitality. She acted as convener for R&D and actively involved in organizing ICRTEMMS-2018 as registration committee Convener. She can be contacted at email: bjd.kalyani@iare.ac.in.

Jaya Krishna Modadugu is working as Software Engineer, Fintech Industry with 8 years of Experience in software development. He has extensive expertise in designing and developing secure, scalable microservices using technologies such as Spring Boot, Java, and cloud platforms like AWS and GCP. Over the course of his career, he has contributed to several mission-critical applications and led key initiatives involving database systems including Oracle, MongoDB, Spanner, and Firestore. He is also proficient in identity and access management using Okta and has played an instrumental role in ensuring application security and compliance. His interests lie in cloud computing, enterprise application development, and distributed systems. He can be contacted at email: jayakrishna.modadugu@gmail.com.

Sarabu Neelima is Dean–Quality Management System and Professor in Computer Science and Engineering, Priyadarshini Institute of Science and Technology for Women (PRIW) is having more than 20 years of academic career in teaching and administration, 7 years of research in Engineering institutions. She obtained her M.Tech. (CSE) from JNTUH in 2011. She has done her Ph.D. research in the field of Data Mining at JNTUH and awarded in 2019. She has guided a number of UG and PG projects. She has 25 publications in journals and conferences at national and international level. Her research work was published in Elsevier, Springer, IEEE, and Scopus. She can be contacted at email: sarabu.neelima@gmail.com.