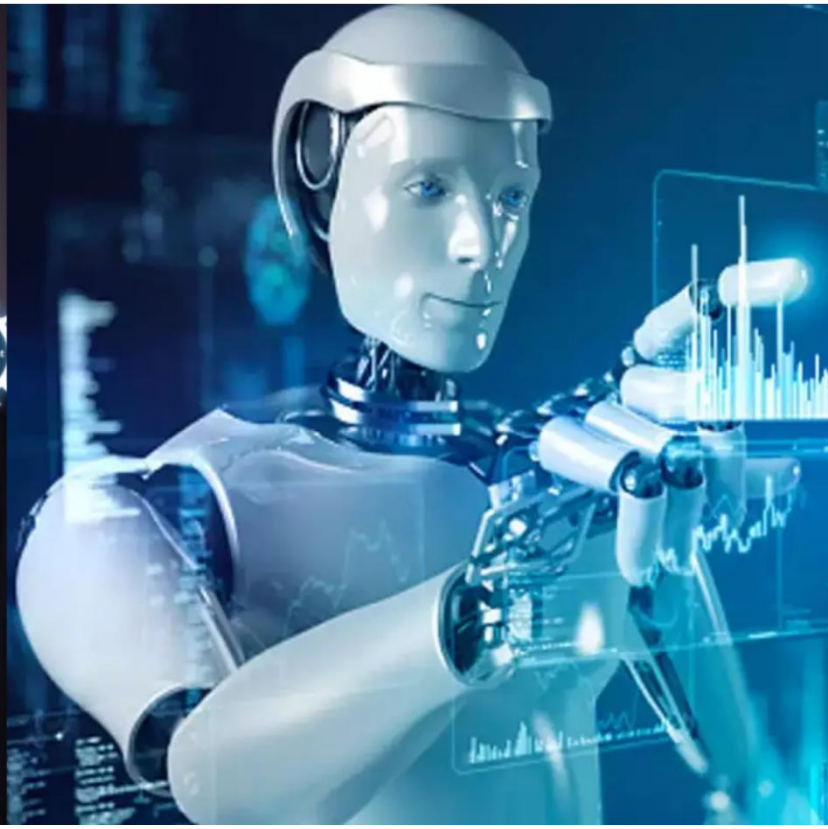
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

E Voting based on Blockchain and Biometric Authentication

Prof.Vedika Patil, Yash Deshmuk, Vijay Chaure, Rohit Jagdale

Assistant Professor, Dept. of CE, KC College of Engineering, Thane, Maharashtra, India

UG Student, Dept. of CE, KC College of Engineering, Thane, Maharashtra, India

UG Student, Dept. of CE, KC College of Engineering, Thane, Maharashtra, India

UG Student, Dept. of CE, KC College of Engineering, Thane, Maharashtra, India

ABSTRACT: The growing demand for safe, transparent and efficient adjustment systems has led to research on advanced technologies such as blockchain and biometric authentication. Traditional coordination methods, including paper-based electronic voting systems, are susceptible to security dates such as voting imports, multiple voting, voice manipulation, and centralized management that can affect the integrity of elections. This article suggests a blockchain and biometric electronic voting system specifically developed for university elections to address these issues. The system integrates biometric authentication to ensure that only legal voters can participate. This means that you can eliminate the risk of fraud and unauthorized access. Blockchain technology is used to provide a decentralized, immutable, transparent voting lid to ensure that the voting process remains manipulated and confirmed. Smart contracts automate voting, reducing the chances of human error and distortion, while ensuring quick and accurate calculations of results. The proposed system will improve accessibility and enable students to coordinate from a secure online platform, while simultaneously maintaining a high level of security and privacy. By eliminating the traditional voting spot and the use of cryptographic encryption technology, the system greatly improves the reliability and reliability of university elections. While challenges such as scalability, biometric data protection, and delays in blockchain transactions must be addressed, the long-term benefits of improving security, transparency and efficiency make this approach to a practical solution for modernizing the voting process.

KEYWORDS: Blockchain, Biometric Authentication, E-Voting, Security, Transparency

I. INTRODUCTION

In modern educational institutions, student elections play an important role in promoting democracy, leadership and student representation. The university's traditional coordination systems, whether paper-based or electronic, are often available for several challenges, including manual errors, voter changes, and logistical inefficiencies. Given the increasing reliance on digital solutions for management procedures, there is an increasing need for safe, transparent and efficient coordination systems that ensure fair elections while maintaining accessibility and user friendliness. To address these issues, the integration of blockchain technology and biometric authentication into electronic voting systems at the university level is a highly effective and reliable solution.

Blockchain technology, known for its decentralized and manipulated nature, provides a secure platform for recording voices on an unchangeable lid. In contrast to centralized databases that can be manipulated or hacked, blockchain ensures that all voting lines-UPs are permanently recorded and unchanged, preventing fraud and voting rights manipulation. This decentralized approach increases transparency as all participants can independently verify election results without relying on central authorities. Additionally, blockchain features intelligent contracts, vote count automation, and results declarations. This eliminates human error and prejudice.

Biometric authentication further enhances the security of the voting process by allowing only registered students to hand over the vote. Traditional ID cards for students or registration based on review methods can easily be misused or shared, leading to cases of voting rights. By using biometric data such as fingerprints and facial recognition, the system carefully checks each voter's identity, prevents unauthorized access, and ensures that each student is correct only once. This not only improves security, but also simplifies the authentication process and makes adjustments more convenient.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

By combining blockchain and biometric authentication, electronic voting systems at the university level can achieve a high level of safety, transparency and efficiency. Biometric login information allows students to vote seamlessly from anywhere on campus, and the blockchain ensures that their voices are safely recorded and counted. This approach not only modernizes the voting process, but also encourages student participation by making it more accessible and reliable. This study examines the architecture, advantages and implementation challenges of blockchain and biometric electronic voting systems, highlighting the potential for revolutionary student elections at universities.

II. PROPOSED SYSTEM

The proposed electronic voting system for university elections integrates blockchain technology with biometric authentication to establish a secure, transparent and efficient coordination mechanism. Traditional adjustment methods, including paper-based and electronic adjustment devices, are equipped with several security challenges, including voter tolerance, voice control and unauthorized access. The combination of decentralized, immutable main register blockchains with biometric authentication obligations ensures a complete voting process that eliminates fraudulent activity and improves voter trust.

The system consists of three important components. A biometric authentication module, a blockchain-based voice book, a user-friendly web or mobile platform for stopping your voice. The voting process begins with a secure voter registration phase in which individual student biometric data, such as fingerprints and face recognition, is securely encrypted and stored. A unique cryptographic hash of biometric data is generated and connected to the student's voter ID, preventing double registration. On Election Day, students will authenticate their identity through biometric authentication before granting access to submit their votes. Because biometric data is unique for each individual, this process eliminates the risk of several votes, voting rights representatives, or identity fraud.

Blockchain technology plays a key role in ensuring the voting process by providing a constant, decentralized, transparent platform for voice storage. As soon as a vote is made, it is encrypted and recorded as a transaction in a blockchain network. In contrast to traditional centralized databases that are susceptible to hacking and operations, blockchain distributes voice records to several nodes, preventing a single entity from modifying or deleting voice. Blockchain immutability prevents the possibility of voting. This means that election results are very safe and reliable. Additionally, blockchain uses cryptographic and zero knowledge evidence (ZKP) to ensure voter anonymity and at the same time maintain the integrity of the election process.

To further improve efficiency, the system uses intelligent contracts, a self-explicit program that produces results that are automatically adjusted and generated after the end of the vocal area. This eliminates manual count errors, reduces administrative workloads, and ensures immediate and operational outcomes. Blockchain transparency allows all involved, including students and electoral officers, to see the voting process in real time, and to promote confidence in the election system.

The proposed system offers many advantages over traditional adjustment methods. By integrating biometrics, we ensure that only legal voters are able to participate, eliminating fraud and identity changes. Blockchain ensures data-based voting security. Additionally, the system improves accessibility by allowing students to coordinate from anywhere on campus, reducing logistical challenges associated with physical voting stands. Auto-counting continues to accelerate the election process and ensure accuracy.

Despite its advantages, the implementation of such a system is challenge-related. Blockchain networks can cause delays in many transactions, which can lead to scalability issues. To improve this, optimized blockchain solutions such as the Layer-2 protocol can be used. Furthermore, data protection concerns related to biometric data storage must be managed in compliance with data protection regulations such as the GDPR. Proper awareness and training for students and administrators is also essentially important for smooth recruitment. The cost of infrastructure may be an issue, but the long-term benefits of a safe and transparent voting process outweigh the initial investment.
Finally, the integration of blockchain and biometric authentication into electronic voting systems at the university level illustrates an innovative approach to conducting secure, transparent and fraudulent elections. The proposed system improves student election integrity and trust among students by eliminating general security gaps such as voter change. Blockchain ensures that all voices are recorded relentlessly and transparently, while biometrics can only participate in legitimate voters.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

III. WORKFLOW OF PROPOSED MODEL

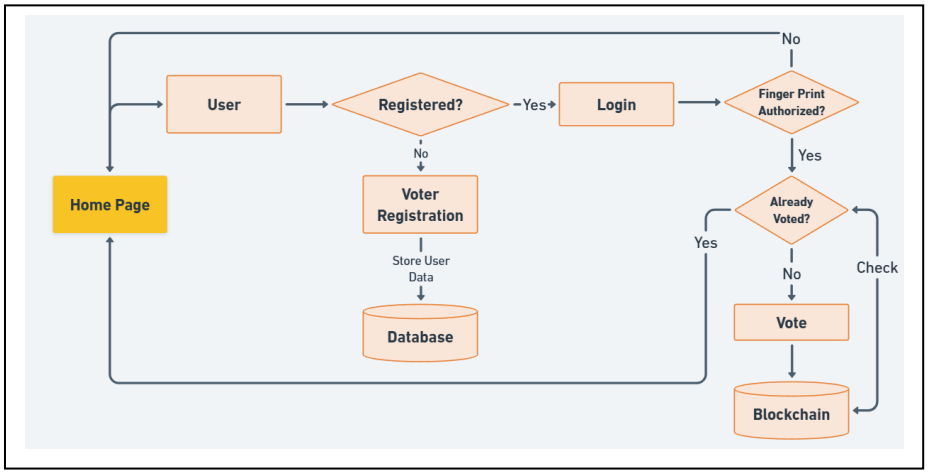


Fig.1 Flowchart

The proposed blockchain and university election biometric electronic voting system workflow follows a structured approach that ensures security, transparency and efficiency at every stage of the voting process. It consists of several important phases, including voter registration, authentication, coordination caste, voting verification, blockchain storage, and declaration of results. Each phase aims to eliminate traditional weaknesses in voting systems, such as: B. It aims to remove unauthorized access, several voting and voting operations, as well as accessibility and trust at the same time.

The process begins with registering the voters. In this process, students register with the system by providing biometric data such as fingerprints and facial recognition. This data is securely encrypted and stored as its own cryptographic hash to ensure that it cannot be replicated or abused. The system connects this biometric hash with a blockchain address that acts as a clear voter-ID for all students. This decentralized approach prevents identity fraud and ensures that only registered students can participate in the election. Multifactorial authentication (MFA) can be included to further improve security. This requires students to verify their identity based on their biometric authentication and on the basis of their registered mobile number or OTP sent to email.

The certification process begins on the correct election day for students. The system asks voters to authenticate their identity with the same biometric login information recorded during registration. The biometric module checks voter identity by comparing the stored cryptographic hash with the provided biometric samples. If authentication is successful, students will access the voting platform so that only legal voters can participate. Because biometric data is clear and cannot be shared or reproduced, this process eliminates the risk of some votes, voter changes, and unauthorized access.

As acknowledged, students can speak up through user-friendly digital platforms. The voting interface contains a list of candidates, and voters select their preferred candidate. After confirming your selection, the system encrypts the vote and records it as a blockchain transaction. Blockchain technology allows each voice to be stored securely in a permanent main register, preventing the possibility of changing or deleting the voice. In contrast to traditional centralized databases that can be manipulated or hacked, the main blockchain book is decentralized and distributed across several knots. This decentralized approach ensures that a single company cannot control or change the recorded voice, and can manipulate and raise the election process.

After the vote, the blockchain network validates the transaction with a consensus mechanism such as: The verification process ensures that the vote is legitimate and free of overlap, and all predefined election criteria are met. After verification, the votes will be stored permanently on the blockchain and are visible for all involved to check. Individual votes will continue to vote anonymously about protecting voters' privacy, but they can publicly check the total number

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

of votes to improve election transparency.

Intelligent contracts are used for automatic vote counts to further improve efficiency and reduce manual intervention. Intelligent Contracts are self-saflin programs that automatically achieve voices and produce results as soon as the voting period ends. Intelligent contracts operate on predefined logic, eliminating the risk of personal errors, manipulation, or bias in the number of votes. Final election results are immediately available on blockchain, providing transparent and verifiable results that students, election authorities and other interest groups can check.

The proposed system workflow offers several advantages over traditional adjustment methods. By integrating biometrics, she ensures that only certified students can vote, preventing fraudulent activities such as multiple coordination and identity changes. Blockchain technology improves security and transparency by creating voices that are constant, verifiable and manipulated tolerant. Using intelligent contracts continues to streamline the voting process, reduces administrative workloads, and ensures fast and accurate results declarations. Additionally, the system improves accessibility by allowing students to coordinate each location on campus, eliminating the need for physical voting stands and reducing logistical challenges.

Despite many advantages, this system also has potential challenges that need to be addressed for a successful implementation. Blockchain networks can cause scalability issues, particularly in a large number of transactions that can lead to delays in voting processing. To mitigate this, optimized blockchain solutions such as the Layer-2 protocol can be used to improve transaction speed and efficiency. Another issue is the secure storage and management of biometric data that meets data protection regulations such as the General Data Protection Ordinance (GDPR) to prevent abuse. The correct encryption techniques and distributed storage mechanisms can help protect voter data. Furthermore, the introduction of users and awareness plays a critical role in the success of the system, requiring educational campaigns and training for students and election officials.

In summary, the proposed electronic voting system workflow integrates biometric authentication, blockchain security and smart contract automation to create a very secure, transparent and efficient voting process for university elections. By eliminating general election choices, this system ensures that student elections are very safe and carried out with greater trust and participation.

IV. DESIGN AND IMPLEMENTATION

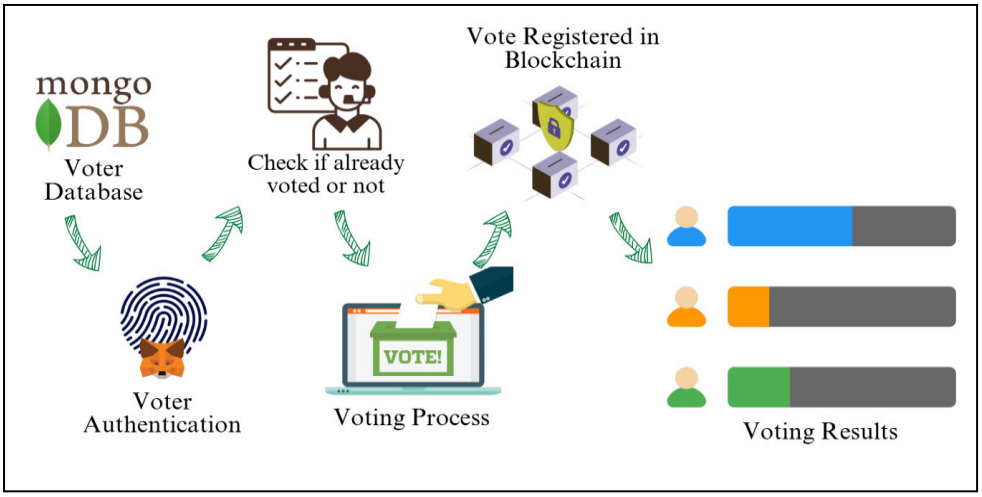


Fig. 2. Design Flow

The design and implementation of the proposed blockchain and biometric-based e-voting system follow a systematic approach that ensures a secure, transparent, and efficient election process.
The project is embedded in a variety of phases, including system design, database and blockchain integration, user interface development, biometric implementation, voting processes, and calculation of results. Each level was carefully

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

developed to remove security gaps, ensuring user-friendly and accessible at the same time for students and election administrators.

The system design phase begins with the definition of the key components required for an electronic voting system. The architecture consists of biometric modules, a blockchain network for storing votes, a secure web or mobile user interface, and intelligent contracts for voting declarations and calculation of results. The authentication module uses biometric registration information to verify the identity of voters, allowing only certified students to hand over the vote. Blockchain networks provide a general book on decentralized, manipulated, operational prevention for recording voices, preventing any form of manipulation or modification. The user interface is intuitive and user-friendly, so students can register, authenticate and choose seamlessly. Intelligent contracts are programmed so that voice verification and counting is automatically performed, eliminating human error and ensuring immediate results declarations.

In the implementation phase, the first step is to register voters. In this step, students will provide biometric data such as fingerprints and facial recognition scans. This data is encrypted and fixed in a distributed database. A unique cryptographic hash of biometric data is generated and connected to a unique blockchain address of the voter. Multi-factor authentication (MFA) can be integrated to improve security. This means that students must verify their identity with the help of biometry and unique passwords (OTPs) sent to their registered mobile number or email.

The voter authentication process begins on the day students try to access the voting system. The biometric module checks voter identity by comparing securely stored hashs from the registration phase with provided biometric samples. If authentication is successful, the voter is granted access to the voting interface. This step eliminates voter risk, some votes, unauthorized access and ensures that only legitimate students will participate in the election.

The authenticated, voice guest process begins. Voters select their preferred candidate from the list that appears on the digital voting platform. After confirming your selection, the vote is encrypted and converted to a blockchain transaction. This transaction is transferred to the blockchain network for verification. The decentralized nature of blockchains ensures that adjustments through several nodes are recorded, preventing the possibility of manipulation and change. In contrast to traditional central databases where voices can be manipulated or hacked, blockchain ensures a common book that all voices remain secure and immutable.

After the adjustment is complete, the verification and storage process takes place. Blockchain nodes validate transactions using consensus mechanisms such as Proof of Authority (POA) and Assignment (POS) to ensure that votes correspond to all predefined election criteria. After verification, the votes are stored permanently on the blockchain, making them publicly verifiable and at the same time maintaining voter anonymity. Cryptographic encryption techniques such as Zero Knowledge Evidence (ZKPS) ensure that you can see the total number of votes, but individual votes are maintained.

Intelligent contracts for automated vote counts are used to ensure a seamless and efficient election process. Smart Contract is a self-appropriate program that automatically votes and calculates election results after the end of the voting period. Intelligent contracts are based on predefined logic, eliminating manual vocal counters and human interference to ensure accurate and fair election results. The final results are publicly available on the blockchain, allowing all involved to see the integrity of their choice. Blockchain transparency ensures that the results are controversial or unchanged, increasing confidence in the voting process.

The system also includes real-time monitoring and testing capabilities that allow students, election officials and administrators to safely track election progress. Blockchain ledgers allow public reviews of vote counts and anonymity for individual voters. This feature increases transparency and prevents all claims of voice manipulation or fraud. Additionally, secure security mechanisms have been implemented to ensure data recovery in technical failures.

Implementation of this electronic voting system offers several advantages over traditional audio methods. Biometric integration ensures that only legal voters can participate, eliminating fraud such as multiple coordination and identity theft. Blockchain technology improves vote security by manipulating election data unchanged. Intelligent contracts automate the voting process, reduce administrative workloads, and ensure immediate and accurate results. The decentralized and transparent nature of blockchain promotes trust among students as it allows independent confirmation

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403311|

of election results. Additionally, the system improves accessibility by allowing it to coordinate with a secure online platform from all locations on campus.

Despite many advantages, this system also presents specific challenges that must be addressed during implementation. Blockchain networks can have delay issues when treating many transactions, which can cause delays in voting processing. To overcome this, optimized blockchain solutions such as Layer-2 scaling protocols can be integrated to improve transaction speed and efficiency. Another important issue is data protection and security, especially with regard to biometric authentication information. The system must comply with global data protection regulations, such as the General Data Protection Ordinance (GDPR) to ensure the secure storage and management of biometric data. Encryption technology and distributed storage mechanisms must be used to prevent unauthorized access to sensitive voter data. Additionally, user training and awareness programs must be implemented to help students and electoral officers become familiar with the new voting system and ensure smooth recruitment. In summary, the design and implementation of blockchain and biometric electronic voting systems follows a structured workflow that integrates modern security features, decentralization and automation. By eliminating the common weaknesses associated with traditional adjustment methods, this system ensures a very safe, transparent and efficient election process for university elections. Challenges such as scalability and data protection need to be managed carefully, but the long-term benefits of improved security, fraud prevention, and the trust of the electoral system make this the ideal framework for modernizing student elections.

REFERENCES

[1] S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, ‘‘E-voting systemusing blockchain technology,’’ in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 113–117, doi:10.1145/3376044.3376062.

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

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

[4] M. S. Farooq, M. Khan, and A. Abid, ‘‘A framework to make charity collection transparent and auditable using blockchain technology,’’ Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106588, doi: 10.1016/j.compeleceng.2020.106588.

[5] N. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ‘‘Blockchain technology—Beyond bitcoin,’’ Sutardja Center Entrepreneurship Technol., Univ. California, Berkeley, CA, USA, Tech. Rep., Oct. 2015. Accessed: Jan. 24, 2018. [Online]. Available: http://scet.berkeley.edu/wpcontent/uploads/Blockchain Paper.pdf

[6] T. Dimitriou, ‘‘Efficient, coercion-free and universally verifiable blockchain-based voting,’’ Comput. Netw., vol. 174, Jun. 2020,Art. no. 107234, doi: 10.1016/j.comnet.2020.107234.

[7] S. Shah, Q. Kanchwala, and H. Mi. (2016). Block Chain Voting System. Economist. [Online]. Available: https://www.economist.com/sites/default/files/northea stern.pdf

[8] S. Park, M. Specter, N. Narula, and R. L. Rivest, ‘‘Going from bad to worse: From internet voting to blockchain voting,’’ J. Cybersecurity, vol. 7, no. 1, pp. 1–15, Feb. 2021, doi: 10.1093/cybsec/tyaa025.

[9] K. M. Khan, J. Arshad, and M. M. Khan, ‘‘Secure digital voting system based on blockchain technology,’’ Int. J. Electron. Government Res.,
vol. 14, no. 1, pp. 53–62, Jan. 2018, doi: 10.4018/IJEGR.2018010103.

[10] C. K. Adiputra, R. Hjort, and H. Sato, ‘‘A proposal of blockchainbased electronic voting system,’’ in Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS), Oct. 2018, pp. 22–27, doi: 10.1109/WorldS4.2018.8611593.

[11] A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers- Plymouth University. Accessed: Feb. 14, 2022. [Online]. Available: https://www.economist.com/sites/default/files/plymout h.pdf

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details