xqrAs per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 03, pages 220-225.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue03.html
DOI: https://doi.org/10.46501/IJMTST1003036

A Secure E-Voting System Using Blockchain Technology

Sujitha.S, Manjunath.K, Amareswar.S, Venkat Lokesh.T, Vijay Kumar.V

Department of Computer Science and Engineering, Kalsalingam Academy Of Research And Education, Anandnagar, Tamilnadu, India

To Cite this Article
Sujitha.S, Manjunath.K, Amareswar.S, Venkat Lokesh.T, Vijay Kumar.V, A Secure E-Voting System Using Blockchain Technology, International Journal for Modern Trends in Science and Technology, 2024, 10(03), pages. 220-225.https://doi.org/10.46501/IJMTST1003036

Article Info
Received: 02 February 2024; Accepted: 26 February 2024; Published: 03 March 2024.

ABSTRACT

This study presents an innovative e-voting system designed to enhance the security, transparency, and integrity of the electoral process by utilizing blockchain technology. The primary purpose of this research is to address the shortcomings of traditional electronic voting systems by leveraging blockchain's decentralized and transparent nature. Methodology-wise, our approach involves implementing a decentralized blockchain network to record and validate votes securely. Each vote is encapsulated within encrypted transaction blocks, forming an immutable chain distributed across multiple nodes. The decentralized structure mitigates the risk of a single point of failure, ensuring resilience against potential attacks. Additionally, cryptographic techniques are employed for voter authentication and identity anonymization, while smart contracts automate the voting process, reducing the risk of human errors and manipulation.

Keywords: E-Voting System, Blockchain Technology,Security, Transparency, Integrity, Encryption

1. INTRODUCTION

The application of blockchain technology to electronic voting offers a revolutionary way to solve the enduring problems with conventional voting methods. The need for a safe, open, and easily accessible voting process is more than ever in today's world when technological innovations are transforming many facets of our existence. The decentralized and distributed ledger architecture of blockchain, which was first created for cryptocurrencies, presents a fresh method for completely altering the election environment.

The fundamental characteristics of blockchain technology, such as its decentralized nature, immutability, and transparency, are essential for enhancing the security and dependability of electronic voting systems. Eliminating the need for a central authority considerably lowers the possibility of manipulation. The blockchain records every vote cast as a block, creating a record that is difficult to tamper with and enhancing the voting process's overall integrity. Because of blockchain's immutability, votes cannot be removed or changed after they are cast, protecting the validity of the results and reducing the possibility of fraud.

Furthermore, it becomes clear that one essential feature of blockchain-based electronic voting systems is transparency. Every member of the network has access to the complete transaction history, which allows for independent confirmation of the accuracy of the outcomes. In addition to encouraging voter trust, this openness serves as a disincentive to any attempt at dishonesty. The use of blockchain technology in electronic voting sticks out as a viable option as we traverse the challenges of contemporary democracy, offering a more inclusive, transparent, and reliable election system going forward.

2. LITERATURE REVIEW

Yichao Lu Huilin Li et. al., This paper likely describes the e-voting system combines blockchain, time-lock puzzles, traceable ring signatures, and time-limited ballot secrecy to create a secure, transparent, and fair electronic voting solution with the ability to prevent fraud, ensure voter anonymity, and maintain the integrity of the voting process. The proposed system is not only theoretically sound but has also undergone practical implementation and evaluation to validate its effectiveness. [1].

G. Revathy K. Bhavana Raj et. al., This paper or article likely explores the concept of the facial recognition component in the proposed voting system is framed as a critical element for ensuring the security, trustworthiness, and inclusivity of the online voting process. Its integration with Blockchain technology signifies a comprehensive approach to address the challenges associated with electronic voting, with an emphasis on minimizing recognition failures and upholding the ethical considerations of privacy and consent. [2].

Junaid Arshad et. al., In this work, the paper contributes to the understanding of scalable blockchain solutions by investigating critical parameters and performance constraints. Additionally, it introduces a novel e-voting system to explore the application of blockchain technology in the voting domain. The structured organization of the paper allows readers to follow a logical flow from the background and related work to the novel contributions and experimental findings. [3].

Vincenzo Agate et. al., This paper introduces Secure Ballot as an electronic voting system specifically designed for supervised elections, with a focus on university elections. Through extensive testing, the system demonstrates high user satisfaction and is asserted to meet all necessary security properties for ensuring user privacy and fair elections. The adaptability of SecureBallot to various supervised election scenarios is highlighted, making it a potentially versatile solution in the realm of electronic voting [4].

Ashkan Emami et. al., This paper introduces an innovative approach to blockchain-based e-voting, emphasizing scalability, privacy, and efficiency. The integration of off-chain computation, specific entities (Ballot Box), and advanced cryptographic techniques contributes to a voting system that addresses key challenges in large-scale elections while maintaining crucial properties and achieving superior efficiency metrics. The implementation and performance analysis on the Ethereum test network provides a practical basis for further research and development in this domain. [5].

3. EXISTING SYSTEM

The existing e-voting system relies primarily on OTP (One-Time Password) verification for securing the electoral process. This system aims to bolster the authentication of voters by implementing a stringent verification mechanism. Each voter is assigned a unique OTP, adding an extra layer of security before they can cast their vote. The integration of blockchain technology further ensures the reliability and transparency of the voting data. Despite these advancements, a notable drawback is the susceptibility of OTPs to phishing attacks. Malicious actors may exploit this vulnerability to trick voters into disclosing their OTPs, jeopardizing the overall authenticity of the voting process. Ongoing efforts to educate voters on secure online practices become crucial in addressing this potential risk.

4. PROPOSED SYSTEM

The suggested method introduces a two-factor authentication architecture that combines facial recognition and OTP verification to overcome the vulnerabilities in the current electronic voting setup. Before voters are allowed to cast their ballots, this dual-layered system improves the voter authentication procedure and overall security. The addition of a biometric component through the use of facial recognition technology makes it much harder for hostile entities to alter or compromise the system. The e-voting process is made more secure by requiring both OTP and facial identification, which also offers a stronger barrier against potential phishing assaults. The goal of this extensive verification process is to lower the risks related to fraudulent activity and unlawful access to build a more robust and dependable electoral system.

5. PROPOSED METHODOLOGY

A. HASHING

A key element in the security of blockchain-based electronic voting systems is hashing. Hashing is a cryptographic technique used in electronic voting that converts input data into a fixed-length character string called a hash value. When voting electronically, every vote is hashed, producing an individual, irreversible representation based on certain characteristics such as the selected candidate and the date. After that, this hash is safely kept on the blockchain, producing an unchangeable record. Hashing's strength is its ability to quickly identify attempts to tamper with the vote data because each modification would result in a unique hash value. By using this method, the blockchain guarantees the transparency and tamper-evident record of the entire voting process.

B. ETHEREUM

Decentralized apps (DApps) and smart contract execution are made possible by Ethereum, an open-source, decentralized blockchain platform. It employs Proof-of-Stake, a consensus technique, to verify transactions and safeguard the network. Ether (ETH), a cryptocurrency that is used for value exchanges and to reward network users, is at the center of it all. One key component is smart contracts, which are self-executing programs with prewritten rules that automate a number of tasks and do away with the need for middlemen. A distributed network of nodes uses Ethereum's blockchain to store the whole history of transactions and smart contract executions. Utilizing Ethereum's Turing-complete programming language, developers can implement their DApps and construct a variety of decentralized solutions, such as non-fungible currencies and decentralized finance (DeFi) protocols.

C.BLOCKCHAIN

Blockchain is a decentralized and secure technology comprised of several essential components. In this innovative system, information is organized into blocks, each containing transaction details and a unique cryptographic hash, and these blocks form an unalterable chain by referencing the previous one. Operating on a peer-to-peer network, blockchain eliminates the need for a central authority, fostering trust and security. Consensus algorithms like Proof of Work or Proof of Stake ensure agreement among participants on the validity and order of transactions. The application of cryptographic hash functions maintains data integrity by creating unique identifiers for blocks. Smart contracts, coded agreements that automatically execute predefined terms, contribute to the efficiency and automation of blockchain applications. Public and private key pairs secure transactions, with the public key serving as an address for receiving funds, and the private key authorizing and signing transactions. Nodes, individual devices on the network, play a crucial role in maintaining the blockchain by validating transactions and contributing to the consensus process. This combination of components provides a transparent, tamper-resistant, and versatile framework applicable to various industries beyond crypto currencies

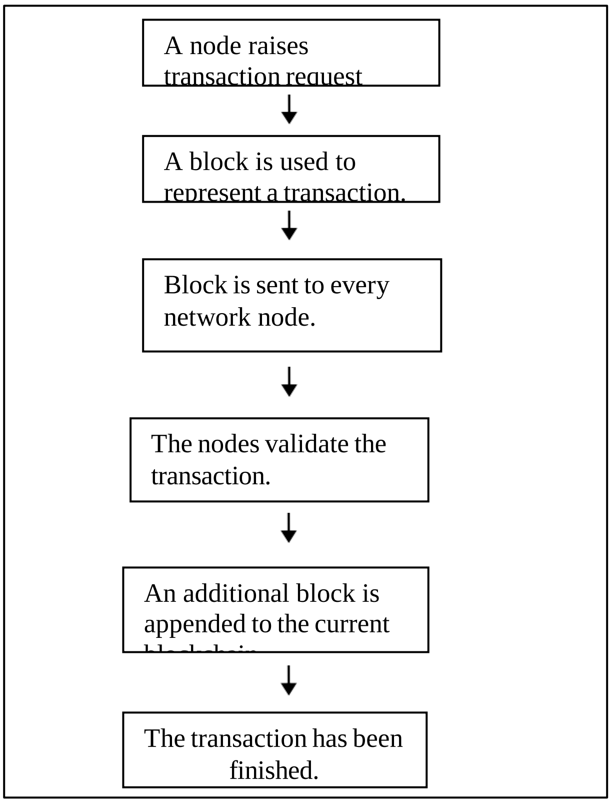

A node raises transaction request
A block is used to represent a transaction.
Block is sent to every network node.
The nodes validate the transaction.
An additional block is appended to the current blockchain
The transaction has been finished.

Fig 1: Working of Blockchain technology

REGISTRATION MODULE

The registration module in e-voting blockchain technology is a critical component designed to authenticate and validate eligible voters before they participate in the electoral process. In this module, each eligible voter is assigned a unique digital identity, typically represented as a cryptographic hash or other secure identifier. This digital identity is securely stored on the blockchain, ensuring tamper-resistant and transparent registration records. The use of blockchain technology enhances the security and integrity of the registration process by providing a decentralized and immutable ledger. This module plays a pivotal role in maintaining the accuracy of the voter registry, preventing duplicate registrations, and ensuring that only authorized individuals can cast their votes. Through the transparent and decentralized nature of the blockchain, the registration module instills trust in the electoral system, fostering a more secure and reliable foundation for e-voting

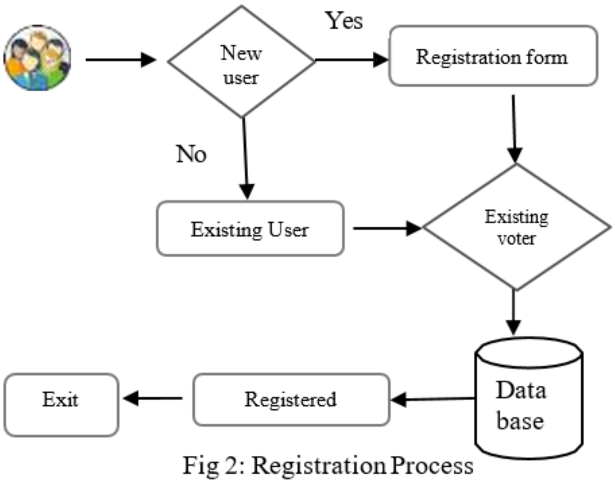


Fig 2: Registration Process

A. LOGIN MODULE

The login module in e-voting blockchain technology serves as the gateway for verified and registered voters to access the voting system securely. During the login process, voters use their unique digital identities or credentials, which were established during the registration phase and securely stored on the blockchain. These credentials may include cryptographic keys, biometric data, or other secure means of authentication. The blockchain ensures the integrity and confidentiality of these login credentials. As voters initiate the login process, the system validates their identity by cross-referencing the provided credentials with the securely stored information on the blockchain. Once authenticated, voters gain access to the voting interface, where they can securely cast their votes. The use of blockchain technology in the login module enhances security by preventing unauthorized access and maintaining a transparent and tamper-evident record of all login activities. This robust authentication process contributes to the overall integrity and reliability of e-voting systems built on blockchain technology.

6. RESULTS AND DISCUSSION

Figure 3 shows the registration module, where a new user can sign up for the procedure and cast a vote in support of it. To prevent duplication, users are only permitted to register once and are not permitted to do so again. The user must complete out a registration form with multiple fields, including name, phone number, email address, and password.

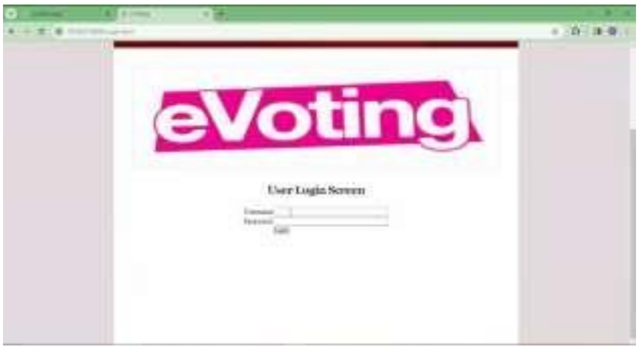
Figure 5 The verification module is visible, where users receive a one-time password on their registered mail addres as soon as they log in. The OTP must be validated before the user may access their particular dashboard.

Figure 7 illustrates the dashboard screen with the electoral symbols of the participating parties displayed. Clicking on one of the symbols casts a vote for the appropriate party. Once a vote is cast, it cannot be repeated, and the user is automatically logged out after a certain amount of time to prevent multiple votes being cast by the same person.

eVoting

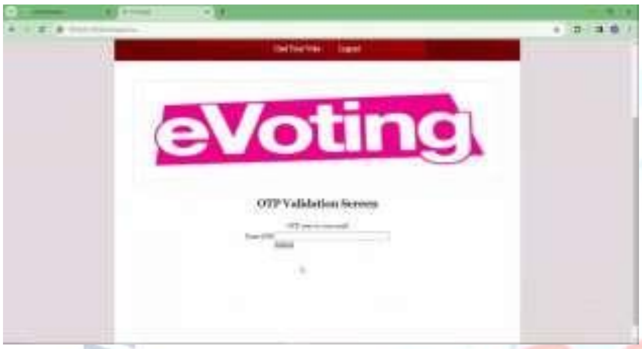
New User Signup Screen

Fig 3: New User Registration Module


eVoting

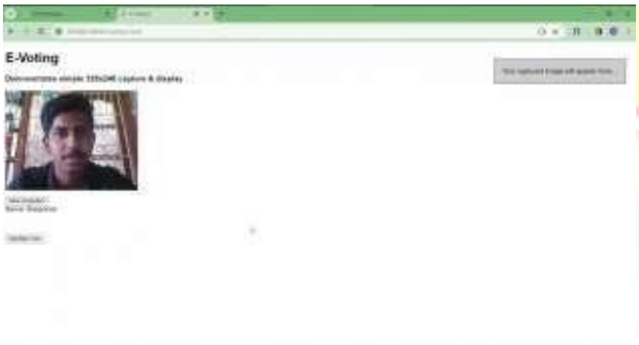
User Login Screen

Fig 4: User Login Screen


eVoting

OTP Validation Screen

Fig 5: OTP Validation Screen


E-Voting

Demonstrates simple 320x240 capture & display

Fig 6: Facial authorization Screen

Figure 6 depicts the Facial authorization screen which enables only authorized users to log in and participate in the voting process.

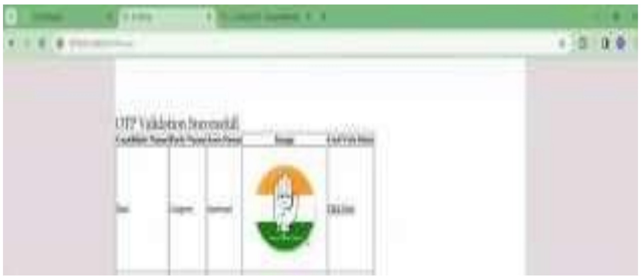

OTP Validation Successful!

Fig 7: Voter Dashboard

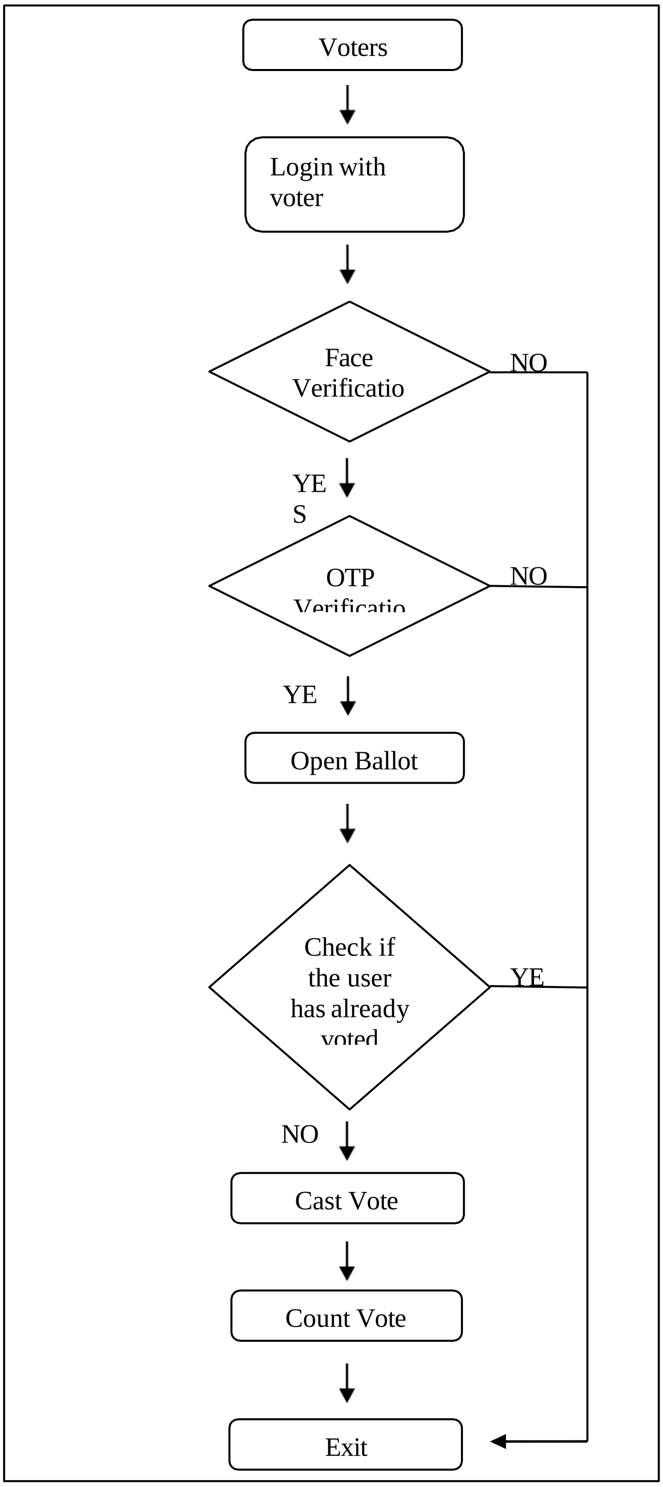


Fig 8: Flow Chart of the voting process

eVoting

Fig 9: Hash Code

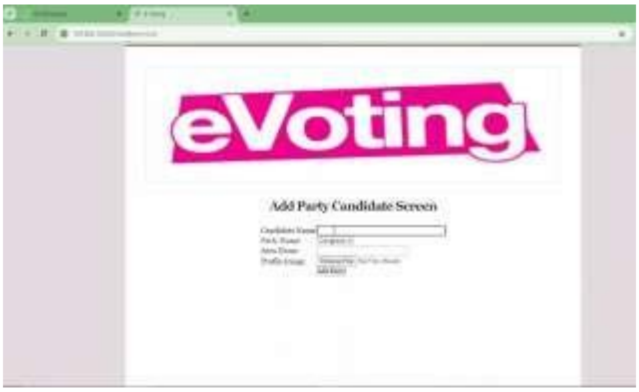


Fig 10: Admin Dash Board

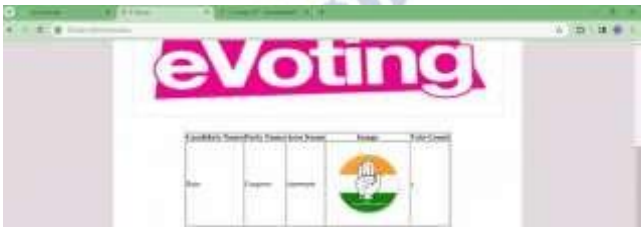


Fig 11: Final Voting Result

Figure 10 and Figure 11 Admin module where the admin can add the party details and view the voting details

Figure 9 shows the process of making new blocks. New blocks are created and sealed the AES-128 method and SHA-256 is used to seal the blocks

7. CONCLUSION AND FUTURE WORK

In conclusion, implementing an e-voting system utilizing blockchain technology and incorporating two-factor authentication presents a promising solution to enhance the security, transparency, and trustworthiness of electoral processes. The decentralized nature of blockchain ensures tamper-resistant record-keeping, while two-factor authentication adds a layer of identity verification, mitigating the risks associated with unauthorized access. This combination not only bolsters the integrity of the voting system but also instills confidence among stakeholders in the accuracy of election results.

Looking ahead, the future scope of this project involves continuous refinement and adaptation to emerging technological advancements. Potential enhancements may include the integration of biometric authentication, improved user interfaces for accessibility, and scalability to accommodate larger voter populations. Furthermore, ongoing collaboration with cyber security experts and regulatory bodies will be essential to address evolving threats and ensure the sustained robustness of the e-voting system.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Yichao Lu, Huilin Li, Hexing Su., "Self-tallying e-voting with public traceability based on blockchain.", Computer Standards & InterfacesVolume 88, March 2024, 103795

[2] G. Revathy, K. Bhavana Raj , Anil Kumar, "Investigation of E-voting system using face recognition using convolutional neural network (CNN)" Theoretical Computer ScienceVolume 925, 10 August 2022, Pages 61-67.

[3] Kashif Mehboob Khan, Junaid Arshad,"Investigating performance constraints for blockchain based secure e-voting system" Future Generation Computer SystemsVolume 105, April 2020, Pages 13-26

[4] Vincenzo Agate, Alessandra De Paola., "SecureBallot: A secure open source e-Voting systemAuthor" Journal of Network and Computer ApplicationsVolume 191, 1 October 2021, 103165

[5] Ashkan Emami.,Habib Yajam," A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations" Journal of Information Security and ApplicationsVolume 79, December 2023, 103645

[6] S. Nakamoto.Bitcoin: A Peer-to-Peer Electronic Cash System, www.Bitcoin.Org, p. 9, 2008.

[7] A. G. Malvik & B. Witzoee. Elliptic Curve Digital Signature Algorithm & its Applications in Bitcoin, pp. 1–5, 2016.

[8] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, & Huaimin Wang3. An Overview about Blockchain Technology: Architecture, Consensus, & Future Trends, IEEE 6th International Congress on Big Data, 2018.

[9] Fridrik p. Hjalmarsson, Gunnlaugur K. Hreidarsson. Blockchain-Based E-Voting System, 2018.

[10] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb. Decentralized Voting Platform Based on Ethereum Blockchain, IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018.

[11] JulijaGolosova, Andrejs Romanovs. Advantages & Disadvantages about Blockchain Technology, 2018 DOI 978-1-7281-1999-1/18

[12] A. Barnes, C. Brake, & T. Perry. Digital Voting with use about Blockchain Technology,Team Plymouth Pioneers – Plymouth University,2016