IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

VotEx Blockchain Portal

[1]Manikandan Ashokkumar, [2]Konar Vembattimuthu, [3]Vignesh Gunasekaran, Krushi Tapasia

[1]B.E Student, [2]B.E Student, [3] B.E Student, B.E Student

[1]B.E in Computer Engineering,

[1]SIES Graduate School of Technology, Nerul, Navi Mumbai, India

Abstract: This document is a model and instructions for LATEX. Online voting is an emerging trend that offers significant advantages, such as reducing organizational costs, increasing voter turnout, and eliminating the need for physical polling stations. However, traditional digital voting systems face criti- cal challenges, including security vulnerabilities, lack of transparency, and susceptibility to manipulation. To address these concerns, blockchain technology presents a decentralized, secure, and transparent solution for electronic voting.

This study explores blockchain-based voting systems, high- lighting their potential to enhance legitimacy, accuracy, safety, and convenience in elections. Blockchain's end-to-end verification, distributed architecture, and cryptographic security make it a strong alternative to traditional voting methods. The proposed system integrates a scalable blockchain framework with flexible consensus algorithms to ensure secure and efficient transactions. The Chain Security Algorithm enhances vote integrity, while smart contracts facilitate secure user interactions. Additionally, cryptographic hashing.

Despite its advantages, blockchain voting faces challenges such as privacy protection and transaction speed, which must be optimized for large-scale adoption. This research presents a performance evaluation of the proposed system, demonstrating its feasibility for large-scale elections. By leveraging blockchain, this approach aims to restore trust in electoral processes, ensuring fairness, transparency, and the protection of democratic rights.

Index Terms **- electronic voting; security; blockchain-based electronic voting; privacy; voting; trust; blockchain technology**

I. INTRODUCTION

Election integrity is essential for preserving voter confidence and accountability in government, as well as for democratic countries. Voters can choose representatives in both corporate and political settings thanks to the voting system, which is essential to political decision-making. Since greater voter participation boosts trust in the democratic process, government everywhere understands the significance of electoral participation. However, public confidence in the voting process is a major factor in how successful elections are.

Conventional paper-based voting procedures, which pro- vide transparency and public trust, have long served as the cornerstone of democratic elections. They do have certain shortcomings, though, such as inefficiency, security problems, and logistical difficulties. The introduction of electronic voting technologies was intended to increase election accessibility, efficiency, and dependability. Blockchain technology has sur- faced as a potential remedy for electronic voting in order to overcome these problems. Because blockchain technology is decentralized, it does not require a central authority, guaran- teeing voting process security, transparency, and immutability. Every vote is documented on a distributed ledger that is impenetrable to tampering, offering improved security, non- repudiation, and end-to-end verifiability. By providing an un- changeable record of votes while preserving voter integrity and privacy, blockchain-based voting systems have the potential to completely transform elections.

This project examines the viability of using blockchain technology for electronic voting by examining its benefits, drawbacks, and possible fixes. The study's goal is to create a transparent, scalable, and safe blockchain-based voting system that tackles important problems including transaction speed, privacy, and accessibility from a distance. The suggested solu- tion aims to rebuild confidence in election procedures and offer a competitive substitute for conventional voting techniques by utilizing cryptographic security, smart contracts, and consensus mechanisms.

II. RELATED WORKS

G. Rathee et al. [1] introduced a blockchain-based digital voting system suitable for technologically advanced environments. But because it presumed that all outside parties were reliable, it was open to security risks. The absence of robust encryption and secure network protocols made it possible for hackers to tamper with votes. On the other hand, our suggested method reduces the likelihood of unwanted access by including strong encryption techniques and secure network protocols. M. Pawlak et al. [2] developed a system that eliminated the need for operating entities but failed to ensure voter identity security. Furthermore, the system needed sophisticated computation, which resulted in latency problems as the user base grew. It thus found it difficult to manage big elections successfully. By employing a flexible consensus mechanism to effectively regulate latency, our suggested approach gets beyond these problems. Additionally, voter identity protection is ensured by cryptographic hashing, which lowers vulnerabilities. D. Chaum et al. [3] proposed an improved voting system with enhanced robustness and fair vote tallying. Voters may verify that their votes were accurately recorded thanks to the system's end-to-end verification feature. But verification necessitated a distinct code input, which made things more complicated. By allowing voters to validate their ballots using registered phone numbers and email addresses, our suggested solution streamlines vote verification while boosting accessibility and confidence. P. McCorry et al. [4] explored an internet-based blockchain voting system without polling stations. Although the study emphasized the promise of blockchain voting, it also pointed up technical issues, such as user duplication errors and system robustness. Low system latency resulted from these problems, but voter privacy was jeopardized. By utilizing smart contracts and a customizable consensus procedure, our suggested system allays these worries while guaranteeing effectiveness and security. Z. Zhao et al. [5] introduced a blockchain-based voting system using homomorphic encryption to preserve voter anonymity. However, their system was hard to scale due of its high processing requirements. Our method uses consensus processes and optimal cryptography to protect voter privacy while preserving computing efficiency. S. Sun et al. [6] developed a blockchain voting system incorporating zero-knowledge proofs (ZKP) for privacy preservation. Their method lengthened the time needed to verify transactions even though it was successful in hiding voter identities. This is improved by our suggested solution, which uses an optimized cryptographic technique to strike a balance between transaction speed and privacy protection. A. Sharma et al. [7] proposed a voting system integrating blockchain with biometric authentication to ensure voter legitimacy. Their strategy, however, sparked questions about user privacy and the security of biometric data. Our technology ensures a secure voting procedure by providing voter authentication through multi-factor authentication (MFA) without sacrificing privacy. L. Hardwick et al. [8] discussed the implementation of a blockchain-based remote voting system but faced challenges related to voter coercion and verification delays. By implementing a tamper-proof audit mechanism and real-time vote veri- fication through secure encryption techniques, our suggested system solves these problems. A. K. Das et al. [9] proposed a hybrid blockchain architecture for voting, combining public and private blockchain layers. This strategy sought to strike a compromise between privacy and transparency. However, when implemented for huge populations, their system was not scalable. By employing a dynamic consensus process that adapts to network load, our suggested architecture improves scalability. S. S. Choi et al. [10] implemented an Ethereum- based voting system utilizing smart contracts for transparency and immutability. However, the approach was costly for large- scale elections because of Ethereum's high gas fees. On the other hand, our method uses alternative blockchain networks with lower computing costs and Unspent Transaction Output (UTXO) models to optimize transaction costs. B. K. Mohanty et al. [11] introduced a decentralized voting system using Hyperledger Fabric. By limiting access to vote data within a permission blockchain, their system enhanced privacy. Permissioned blockchains, however, reintroduce the problems of centralization by requiring faith in the controlling authorities. By keeping a public blockchain and using cryptographic hashing to protect voter anonymity, our approach gets beyond this restriction. E. Alexopoulos et al. [12] explored a zero- knowledge proof (ZKP) approach for blockchain-based voting to ensure voter anonymity while maintaining verifiability. ZKP implementation increased computing burden, notwithstanding its effectiveness. Our system uses scalable network architecture and effective encryption algorithms to strike a compromise between privacy and performance.

III. PROPOSED FRAMEWORK OF VOTING SYSTEM

Unlike other programming frameworks that allow an admin- istrator to add, remove, or update data, blockchain is mutable. Anybody with access to the system can alter or remove the votes if such a system is used for voting. A node cannot be changed or removed from the chain after it has been inserted. If a node is attacked by an intruder, the corresponding nodes detects it and rebuild the damaged node, hence the chain becomes immutable. Because the blockchain is decentralized, no single computing node can influence the voting process. The voting activity remains operational even if any one or more nodes get attacked or become unavailable. It guarantees dependability in every harsh circumstance. Voters, the Election Commission's Administration Authority, and Identification Authorities are the primary stakeholders in the proposed framework.

A. Voting System Architecture

The suggested system's high-level architecture has been shown. It demonstrates how the primary participants Voters, VMS, AA, and IA—cooperate to carry out specific voting duties. Via dAPP, which might be a web portal or a mobile application, all voters have direct access to VMS. Voters who register in the system are verified by the identity authority. Voters may participate in the application process if they are verified as eligible to vote. The first component of the entire system's operation is the application's user interface, which also needs front-end security. The user submits his credentials on that interface, it is crucial that it be easy to use and safe. The first component of the entire system's operation is the application's user interface, which also needs front- end security. Because the user submits his credentials on that interface, it is crucial that it be easy to use and safe. Every user has fair and complete access to the system when voting. Additionally, it offers traceability following voting. Using his credentials, the voter registers in the system. To register a voter in the system, VMS uses their ID information and compares it with IA's online records. A special OTP is sent to the user so they may access the system.

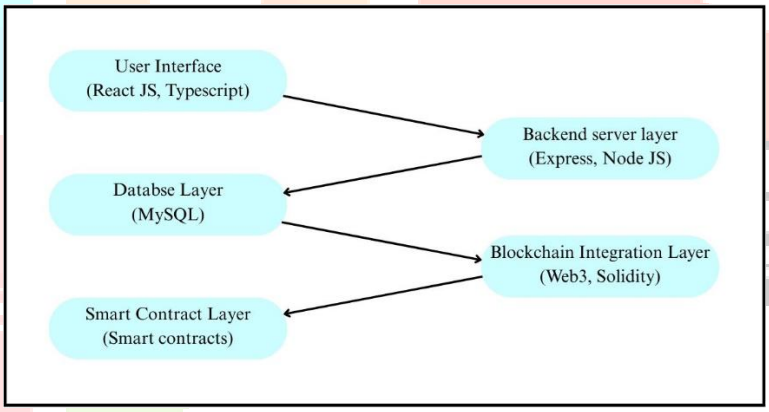

Fig. 1. System Block Diagram

B. Workflow of Proposed Model

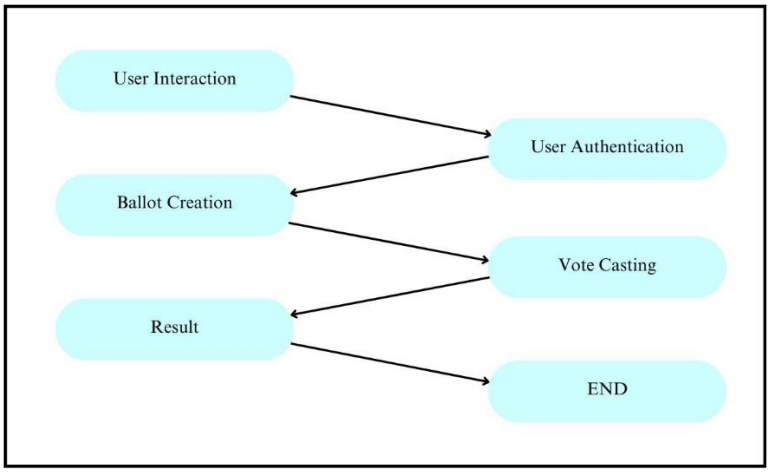

Fig. 2. Flow chart

Following verification, the voter registers in the Voting Management System. The blockchain is used to construct a single chain system. To maintain the integrity of the voting process, the technology is also integrated with the nation's national database. A transaction is created using the voter's national identification number for each vote. The transaction is then mined by the minors and saved in the blockchain. The voter also uses the Vote Coin in his or her wallet when casting the ballot. Once one vote coin has been used, the voter is unable to cast another vote. The voter is taken to the election interface, where all of the candidates running in his or her constituency are displayed, after logging in with their credentials. When a voter requests to vote, VMS compares the voter's computerized National ID with all transaction hashes that already exist on the blockchain to confirm the voter's voting status. VMS will reject the request and remove the voter from the system if a transaction hash is discovered that matches the voter's computerized National ID. If a voter has not voted yet, the request is transferred to the miner to add the node. After choosing his preferred candidate, the voter casts his ballot. The miner executes the transaction and keeps track of it with the use of transaction hash. After then, the node is included in the balloting chain. To cast a ballot, voters need to have access to a smartphone or web browser. To make it user-friendly for all users, the voter interface would be available in multiple languages. At the time of voting, a sizable number of voters may be present under the suggested approach. Voters can cast ballots from anywhere in the world thanks to a decentralized blockchain technology. Voting can be done from anywhere, including abroad, as long as the voter's digital national identification is validated, in this way his/her computerized National ID is verified from the national database so he can cast the vote. After being delivered to a pool, voting transactions are examined by miners, who then eliminate fraudulent requests by obtaining consensus from other nodes before adding them to the chain. A cryptographic hash ensures the votes are completely safe. A new block is added to the chain with each vote. Additionally, the system ensures that a single user can only cast one vote using the vote coin. The method makes guarantee that no voter casts two votes, even if there is a technical issue that prevents the voting coin's balance from being updated. By verifying if a transaction hash is created using the voter's computerized national ID, the miner can determine whether any voter requests or nodes are malicious. An SMS is sent to the voter's registered phone number and email address upon the completion of the transaction and the successful addition of a node to the Vote Chain. By providing a unique transaction hash, the voter can use a web portal to confirm his vote. Once the transaction is properly completed, the vote is counted in the entire voting process. When a voter casts a ballot successfully, there are zero vote coins in the voter wallet. the utilization of outside sources, the Application Layer offers a user verification system. It serves as the voting system's main user interface. It stores the voting system's data in internet databases. This layer also manages all blockchain transactions. The user's eligibility to participate in this voting activity is confirmed by his or her national ID.

C.Layered Structure of the Proposed VMS

A layered structure has been used to demonstrate the suggested framework. The process of system services has been divided into five tiers, which are displayed as follows. All of the dAAPs created for administration and voters are included in the interface layer. Any stakeholder can connect to VMS via these distributed applications.

D. Some Common Mistakes

Security Vulnerabilities: Weak Authentication Measures: If the OTP system is not implemented securely, it can be vulnerable to interception or phishing attacks. Lack of Encryption: Storing or trans- mitting voter credentials and voting data without strong encryption can lead to data breaches. Insufficient Front-End Security: The user interface must be protected against common threats like cross-site scripting (XSS) and SQL injection.

Voter Registration Issues Inaccurate Voter Verification: If the Identification Authority (IA) database is outdated or incorrect, eligible voters may be denied access, or fraudulent users may get registered. Scalability Problems: If the system is not designed to handle a high number of voters at once, it may experience slowdowns or crashes during peak voting times.

Voting Coin (VC) Mismanagement Loss or Du- plication of Voting Coins: Errors in allocation or transaction handling could lead to situations where a voter is unable to vote or where duplicate votes occur. No Recovery Mechanism: If a voter loses access to their Voting Coin due to a system issue, there should be a mechanism for recovery without compromising security.

Absence of Auditability and Transparency Lack of a Clear Traceability Mechanism: Election results disputes may arise if votes cannot be accurately tracked without disclosing voter identities. Limited Voter Confirmation: Voters should be able to verify that their vote was cast and accurately counted using the system.

User Experience (UX) is poor. Create Complex User Interface: Voters may become frustrated and contribute less to the system if the user interface is difficult to use. Problems with Device Compatibility: To guarantee accessibility for all voters, the dApp should function flawlessly on a variety of hardware and operating systems.

Legal and Regulatory Non-Compliance Ignoring Election rules: The system needs to abide with local election rules, such as those pertaining to voting standards and data protection. Absence of Security Audits: To find and address vulnerabilities before they can be exploited, regular security audits and penetration tests should be carried out.

E. Figures and Tables

The "VotEx Blockchain Portal" interface enables users to vote by selecting candidates, viewing their details, and casting votes securely on a blockchain system. It also allows admins to add candidates, set election dates, and manage e-voting, ensuring a transparent and efficient election process.

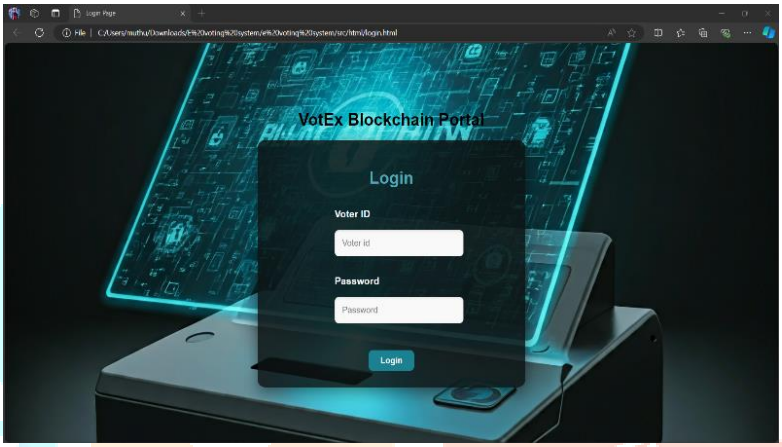

Fig. 3. Login page of the website

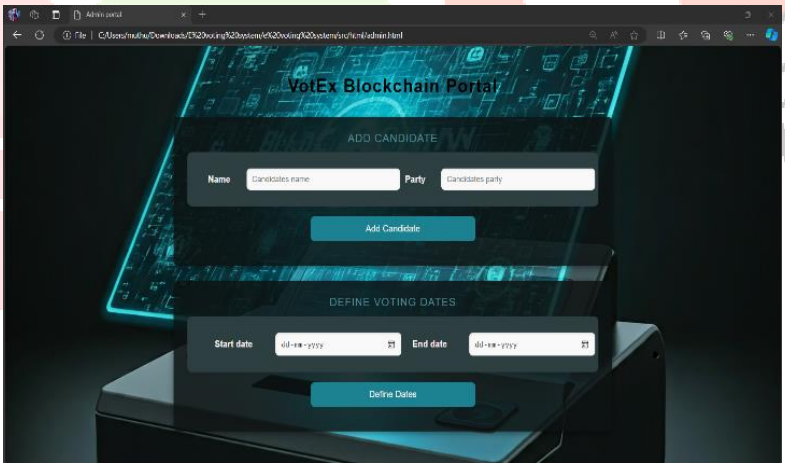

Fig. 4. Admin page of the website

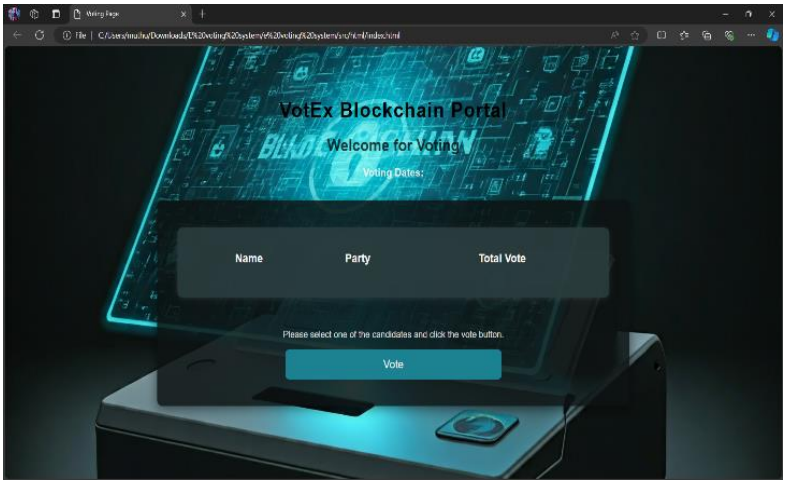

Fig. 5. Voting Page of website

IV. ACKNOWLEDGMENT

We sincerely appreciate the invaluable guidance, continuous support, and insightful feedback provided by our mentor, Rasika Malgi Ma'am, throughout this research. Her expertise and encouragement have played a crucial role in shaping the direction of our study. We are also thankful to the faculty and staff of SIES Graduate School of Technology, Mumbai, for equipping us with the necessary resources and creating a supportive environment that facilitated our research. Additionally, we extend our gratitude to our peers and colleagues for their valuable discussions, suggestions, and assistance during this project. Their insights have significantly contributed to refining our approach and strengthening our findings. Lastly, we would like to express our deep appreciation to our families and friends for their unwavering encouragement and motivation, which have been a constant source of strength throughout our research journey.

REFERENCES

[1] "Online Voting System Using Blockchain" Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure, Pranali Shirke and Prasad Halgaonkar.

[2] "Scalable Blockchain Based Electronic Voting Systems" Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur and Hafiz Adnan Hussain.

[3] "Blockchain Based on E-voting Systems" Yousif Osman Abuidris, Rajesh Kumar and Wang Wenyong.

[4] "Voting System using Blockchain Technology" Mayur Shirsath, Mohit Zade, Riteshkumar Talke, Praful Wake and Maya Shelke.

[5] "Smart Electronic Voting System Using Blockchain Technology" Naina Nagesh Dhepe and Dr. Pathan Mohd Shaf.

[6] Abhishek Subhash Yadav, Yash Vandesh Urade. Ashish Utamrao Thombare, Abhijeet Anil Patil, 2020, E-Voting using Blockchain Technology, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 07 (July 2020), DOI: 10.17577/JERTV9JS070183.

[7] G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018,00151, keywords: Contracts: Electronic voting:Peer-to-peer computing: Privacy: Electronic voting systems, Blockchain:E-Voting: Voting, Smart Contract Private Blockchain.

[8] Hajian Berenjestanaki. M.; Barzegar, H.R.: El loini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. Electronics 2024, 13, 17.