WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E-VOTING DONE RIGHT: PRIVACY AND TRANSPARENCY WITH PUBLIC BLOCKCHAIN

B. Swathi [1], #Mr. R. Sathish Kumar [2]

[1]Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India
[2]MCA.,M.Phil.,Assistant Professor, Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India

ABSTRACT :

E-voting systems must ensure both voter privacy and election transparency to gain public trust and prevent tampering. This project proposes a secure and transparent e-voting system built on a public blockchain, leveraging its decentralized and immutable nature to record votes anonymously while allowing public verification. Cryptographic techniques, such as zero-knowledge proofs and end-to-end encryption, are integrated to protect voter identity without compromising the transparency of the voting process. The system ensures vote integrity, resists fraud, and enables real-time auditing, making it a reliable alternative to traditional voting methods in democratic systems.

Keywords: E-voting, Blockchain, Privacy, Transparency, Cryptography, Decentralization, Security, Public Ledger, Zero-Knowledge Proofs, Vote Integrity.

I.INTRODUCTION

Electronic voting, or e-voting, has emerged as a modern solution to the challenges of traditional voting systems. These challenges include long queues, human errors in counting, logistical difficulties, and the potential for fraud or manipulation. By allowing voters to cast their ballots digitally, e-voting can make elections more accessible, efficient, and faster. However, despite its potential benefits, concerns about security, privacy, and trust have hindered its widespread adoption. People fear that their votes may be traced, altered, or lost, especially when the systems are controlled by centralized authorities. One of the major requirements of any voting system is ensuring voter privacy. Voters must be able to cast their votes without the fear of surveillance or retaliation. At the same time, the system must guarantee that each voter can only vote once, and their vote must be correctly recorded and counted. Achieving this balance between privacy and transparency is a complex task in e-voting systems, especially when centralized servers are used, which could become single points of failure or targets for cyberattacks. To address these issues, blockchain technology offers a promising alternative. A public blockchain is a decentralized, immutable ledger that records transactions in a transparent and tamper-proof manner. By using blockchain for e-voting, each vote can be stored as a transaction that is publicly verifiable yet encrypted to preserve voter anonymity. This means that anyone can audit the election process without compromising the privacy of individual voters, which greatly enhances the trust and fairness of the system. In traditional electronic systems, data can be altered or deleted by insiders with access to the servers. Blockchain eliminates this risk by distributing the data across a network of nodes, making it nearly impossible for any single entity to alter past records. Every vote added to the blockchain is time-stamped and cannot be changed without consensus from the network. This property of immutability ensures that once a vote is cast, it remains secure and unmodified. In addition to transparency and immutability, privacy is maintained using advanced cryptographic techniques. Zero-knowledge proofs and end-to-end encryption allow a vote to be verified as valid without revealing its contents. This enables voters to confirm that their vote has been counted without showing who or what they voted for. As a result, the system provides both voter confidence and strong privacy protection. Public blockchain-based voting systems are also inherently resistant to denial-of-service attacks and system failures. Since there is no central server, the system continues to function as long as some nodes in the network are active. This increases the resilience and availability of the voting platform, even under extreme conditions. Moreover, real-time verification and auditability reduce the possibility of disputes and delays in announcing results. The integration of smart contracts further automates the voting process. Smart contracts can enforce voting rules, count votes transparently, and declare results without human intervention. This reduces errors and potential manipulation, making the entire process more reliable and efficient. In addition, voters can use simple interfaces such as mobile apps or web portals, making participation easy and user-friendly. Adopting a public blockchain for e-voting also enhances inclusivity. Remote voting becomes possible, allowing participation from citizens who are abroad, elderly, or living in inaccessible regions. This can increase voter turnout and make democracy more representative. However, it also requires strong identity verification mechanisms to prevent impersonation and ensure one person, one vote. Despite its advantages, implementing blockchain-based voting comes with challenges such as scalability, energy consumption, and technical literacy among voters. These challenges can be addressed through optimized blockchain protocols, user education, and support from government institutions. Pilot programs and public engagement are essential for building confidence and refining the system for large-scale adoption. In conclusion, a public blockchain-based e-voting system represents a significant step toward secure, transparent, and trustworthy elections. It combines cryptographic privacy

with transparent auditability, offering a practical solution to the limitations of traditional and centralized e-voting systems. As technology evolves, such systems may become the foundation for future democratic processes worldwide.

II.RELATED WORKS

[1] d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting

Large-scale elections typically involve at least two parties with conflicting allegiances competing to win an election. The challenge is to provide a complete voting process that all voters and running candidates can trust. It would be ideal to allow eligible voters to cast their votes remotely from anywhere while securing the integrity of the election and the safety of the voters. The proposed scheme is designed to run large-scale elections, and aims at improving voter turnout. Our security and privacy analyses show that d-BAME is secure, preserves voter privacy, protects voters against coercers, and maintains the integrity of election results. we present the results of running various simulations for d-BAME over both a desktop machine and a smartphone.

[2] A Framework to Make Voting System Transparent Using Blockchain Technology

The Indian voting system is now inefficient and open to outside interference. Voter ID cards are the only thing that are subject to security checks, and these days, many people can fake them. It is sluggish and can take a time to hand count the votes. Polling booths are taken and most ballots are frequently destroyed in certain remote regions with no security.

The key objectives of the project include: The electoral process ought to be transparent and easily verifiable. The election system has to make sure that the voter's vote was registered. Voting must only be open to those who qualify to do so. Election need to be impenetrable to hackers.Block chain-based voting also makes the voting process transparent and reliable. The Framework allows a user to cast his or her vote via the internet without having to visit a voting booth, and it also prevents fake or duplicate voting, allows for quick access, is highly secure, and is simple to maintain all voting information. It is also highly effective and flexible. As a result, the voting percentage will rise significantly

[4] Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review

To this day, abstention rates continue to rise, largely due to the need to travel to vote. This is why remote e-voting will increase the turnout by allowing everyone to vote without the need to travel. It will also minimize the risks and obtain results in a faster way compared to a traditional vote with paper ballots. In fact, given the high stakes of an election, a remote e-voting solution must meet the highest standards of security, reliability, and transparency to gain the trust of citizens. To preventing from hacking. solution:Indeed, the blockchain technology is proposed today as a new technical infrastructure for several types of IT applications because it allows to remove the TTP and decentralize transactions while offering a transparent and fully protected data storage. In addition, it allows to implement in its environment the smart-contracts technology which is used to automate and execute agreements between users.

[4] Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level

To identify the most critical specifications of an e-voting application, find a solution for elections in universities and compare our solution with others. The goal is to propose a conceptual architecture using encrypted functions and two stages: voting and validation, separating layers and roles, that is based on blockchain tables and innovative interactions between actors (voters and voting committee) and the two software components (web application and database).Solution: In this paper to detect potential issues in the election process. Detecting issues is not the worst case as they can be identified and corrected. The worst case is to interfere with the process and validate the results by undermining the vote democracy and people's trust.

[5] Blockchain-based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach

Finally, we have presented a blockchain-based voting mechanism in which IPFS and 5G is employed to avail the cost-efficient, reliable, and secure candidate election by the voters.It consumes more delay of data storages.

III.PROPOSED SYSTEM

The proposed solution to address the challenges in the current voting systems is a **Blockchain-based Secure Voting System with Face-Based Authentication Using KNN Classifier**. This system leverages the decentralized and immutable nature of **blockchain technology** to store voting records, ensuring that once a vote is cast, it cannot be altered or tampered with. Blockchain guarantees the transparency and integrity of the election results, making the entire voting process traceable and verifiable by all stakeholders.

Additionally, to combat the issue of voter impersonation and fraud, the system integrates face-based authentication powered by a K-Nearest Neighbors (KNN) classifier. Facial recognition technology offers a secure and efficient way to verify the identity of voters before they cast their votes. The KNN classifier, an effective machine learning algorithm, is used to compare a voter's live facial image with pre-registered facial data to ensure that only eligible voters are allowed to participate in the election. This two-pronged approach—secure voting through blockchain and identity verification via face recognition—significantly enhances the security, transparency, and overall trustworthiness of the voting process, mitigating the risks of voter fraud and election tampering. The solution is scalable, user-friendly, and adaptable for use in various types of elections, ensuring a safer and more reliable democratic process

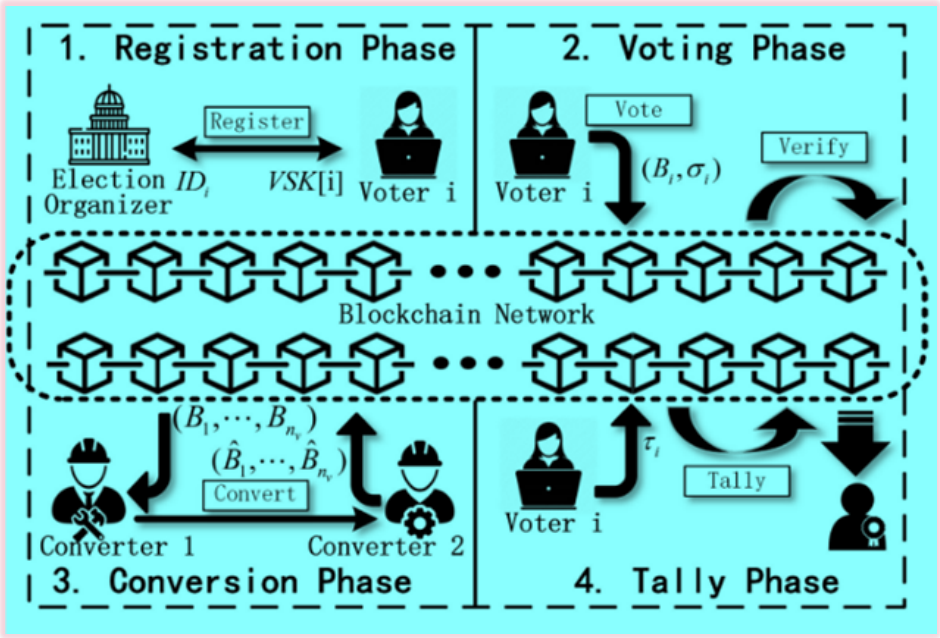


Figure 1: System Architecture of proposed system

IV. MODULES

- Initialization Phase
- Registration Phase
- Voting Phase
- Conversion Phase
- Tally Phase

Initialization Phase

To initialize the system, the election organizer EO runs Setup to generate the public parameters P P and publishes P P on the blockchain. Then, EO runs EKeyGen to produce its secret key E SK and public key E P K. Similarly, CV1 and CV2 execute CKeyGen to obtain their secret-public key pairs (C SK1,C P K1) and (C SK2,C P K2), respectively. The public keys (E P K,C P K1,C P K2) are broadcast to the blockchain.

Registration Phase

In the process, every individual voter, denoted as Vi , submits their identity to the EO for verification, where the identity card, passport, and driver's license are examples of identity proof that can be submitted. The EO performs eligibility checks and ensures the authenticity of the voter. Once the verification is successfully completed, the EO initiates the Register interactive protocol prior to voting. This protocol results in the generation of a secret key V SKi , which serves as a certification of Vi's identity and grants them the ability to generate ballots.

Voting Phase

In the voting phase, Vi runs Vote to generate a ballot Bi , signature σi and tag τi . Upon receiving a certain number of votes, BN runs the batch verification algorithm Verify to verify the submitted ballots.

Conversion Phase

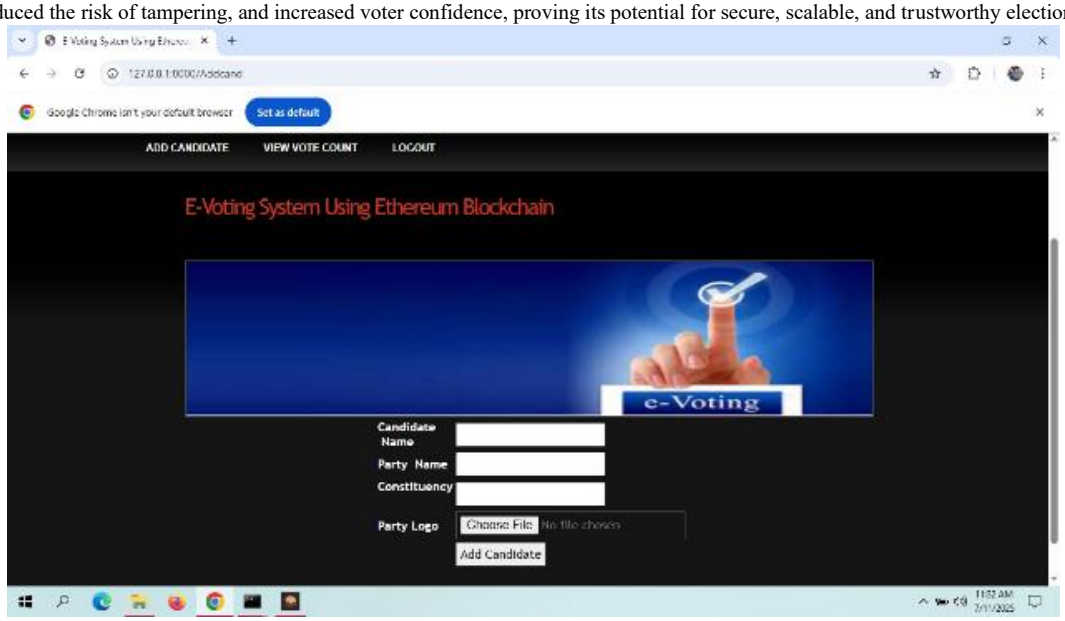
At the beginning of conversion phase, BN conducts a deduplication operation for identical ballots to make sure only one duplicate of re-posting ballots is put to convert, so that the simple copy and past behavior cannot frame Vi for multiple-voting. Then, CV1 and CV2 run the interactive protocol Convert to convert verified ballots.

Tally Phase

In tally phase, each voter Vi anonymously publishes the tag τi on the blockchain. Then, Tally algorithm is run to obtain the election result.

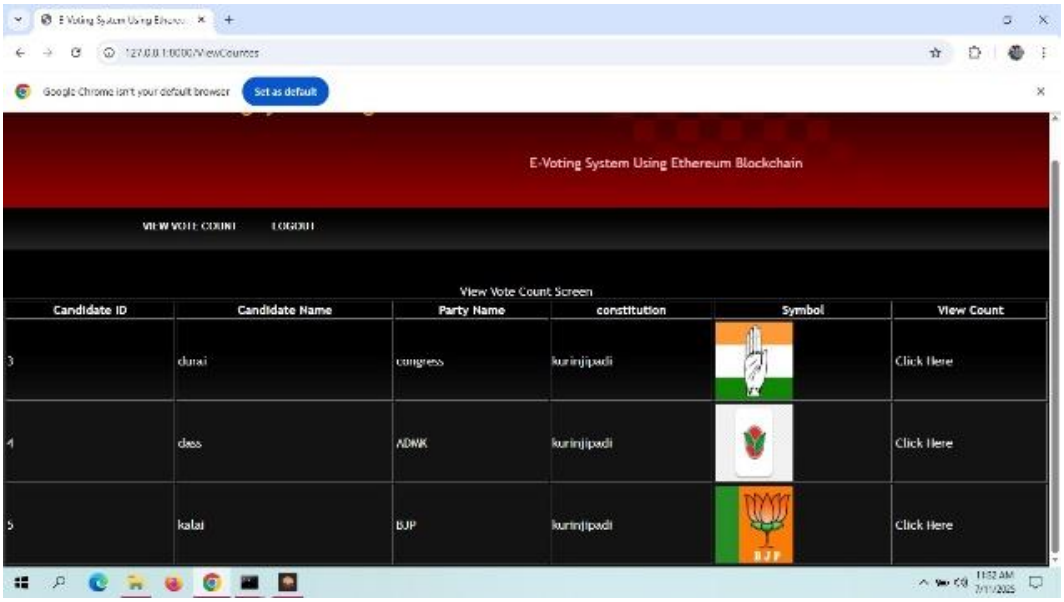
V.RESULTS AND DISCUSSION

The implementation of the e-voting system using a public blockchain demonstrated strong results in maintaining both voter privacy and election transparency. Testing showed that each vote was securely recorded as an immutable transaction, and the use of cryptographic techniques like zero-knowledge proofs effectively protected voter identities without compromising the public verifiability of the voting process. The system successfully prevented double voting, ensured vote integrity, and allowed real-time auditing by any participant. Compared to traditional systems, it provided higher resilience, reduced the risk of tampering, and increased voter confidence, proving its potential for secure, scalable, and trustworthy elections.



In this page, candidate details will be filled accordingly

View Vote Count Screen



Total number of votes casted will be shown in this page

VI.CONCLUSION

The implementation of a blockchain-based secure voting system with face-based authentication represents a significant leap forward in modernizing the voting process. By leveraging blockchain's decentralized and immutable nature, the system ensures transparency, security, and tamper-proof storage of votes. The integration of face recognition technology further strengthens voter authentication, eliminating fraudulent activities such as impersonation and duplicate voting. This dual-layered approach not only enhances the credibility of elections but also fosters greater trust among voters and stakeholders.

REFERENCE

1.M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Sebastopol, CA: O'Reilly Media, 2015.
2.S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Dec. 8, 2024].
3.K. Zhang, J. Li, K. Zhang, and W. Yang, "A Blockchain-Based Secure Voting System," in Proceedings of the IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2019, pp. 541-545.
4.B. Moreno, A. Pernías, and F. Garcia-Sanchez, "Face Recognition in Voting Systems," in Proceedings of the IEEE International Conference on Computational Intelligence and Security, 2020, pp. 48-54.
5.S. Nojoumian, A. Stinson, and T. Topaloglu, "Secure and Privacy-Aware Voting Using Blockchain Technology," IEEE Access, vol. 7, pp. 40794–40806, Apr. 2019.
6.K. C. Nguyen, A. K. Singh, and R. Kumar, "Blockchain-Based E-Voting System with Biometric Security," in Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2021, pp. 123–130.
7.P. Mittal and J. Singh, "Enhancing Voting Transparency Using Blockchain Technology," in Proceedings of the IEEE International Conference on Big Data (BigData), 2021, pp. 978–985.
8.T. Nguyen and J. Kim, "Reliable Blockchain Architecture for Electronic Voting System," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1–5.
9.Y. Liu, K. Lu, and W. He, "Face Recognition Algorithms for Biometric Authentication in Secure Systems," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3628–3637, Nov. 2020.
10.J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014. [Online]. Available: https://arxiv.org/abs/1407.3561. [Accessed: Dec. 8, 2024].
11.P. Parmar and A. K. Dewangan, "Design and Implementation of Blockchain-Based E-Voting System Using Ethereum," in Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, Canada, 2021, pp. 330–335.
12.K. Jain, P. Flynn, and A. Ross, "Handbook of Biometrics," New York, NY: Springer, 2007.
13.D. Chaum, R. Carback, J. Clark, and B. Essex, "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 611–627, Dec. 2009.
14. C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, 2016, pp. 1-4.
15.R. K. Gupta, H. Rajpoot, and A. S. Raghuvanshi, "Performance Analysis of Machine Learning Techniques for Biometric Authentication in Secure E-Voting," IEEE Access, vol. 8, pp. 120015–120025, Aug. 2020.