International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE AND TRANSPARENT E-VOTING SYSTEM USING BLOCKCHAIN, SMART CONTRACTS, DIFFERENTIAL PRIVACY, AND EMAIL-BASED VOTER AUTHENTICATION

D. KRISHNA VENI [1], DAYALA VARSHITHA [2], SAI LIKITHA BHIMANATHUNI [3], PENDEM ANVESH [4], MARAM REDDY SREEKAR REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Election is the key process typically utilized for maintaining democracy in a given society. Recent technological advancements, such as Blockchain (BC), have been already deployed in previous works to realize non-conventional e-Voting systems. The main goal for such proposals is to provide the necessary level of security and reliability, while maintaining transparency, trust, and remote elections. However, the distributed and publicity nature of BC brought new challenges related to privacy and performance trade-off. This paper aims to address existing privacy and performance issues in e-voting by integrating smart contracts for reliability and transparency, Differential Privacy to enhance vote anonymity, and Self-Sovereign Identities (SSI) for managing decentralized identity and verifiable credentials. Specifically, a novel (k, ε)-differential privacy mechanism is developed, in which a randomly selected candidate is used as a pivot to redistribute retrievable votes to other candidates, preserving anonymity while enabling statistical vote approximation. To enhance user interaction, the system also includes a real-time notification mechanism that sends a confirmation message—such as "Vote successfully cast"—to the user's registered

mobile device upon completing the voting process. The proposed methods are evaluated under various conditions, including different transaction arrival rates (10–80 TX/s), total cast votes (10k–50k), and numbers of elected candidates (2–8). To validate its practical deployment, the smart contract is implemented on a cloud-hosted, permissioned blockchain network using Hyperledger Besu, with geographically distributed nodes in Google's EU and USA data centers. Experimental results indicate that BP-Vot achieves a 24% improvement in latency over existing solutions (≈ 1 s/TX vs. 1.24 s/TX). Moreover, through a standardized Min-Max regression method, the system consistently delivers over 98% accuracy in approximated vote results, with accuracy improving linearly with vote volume. The proposed differential privacy model is also formally verified to be resilient against reconstruction attacks.

Index Terms – E-Voting, Blockchain, Smart Contracts, Differential Privacy, Voter Authentication, Election Security, Data Privacy, Distributed Ledger Technology, Cryptography, Transparency.

I. INTRODUCTION

Voting has been a critical tool for maintaining democracy worldwide throughout history. Traditionally, voting proce dures are classically performed using centralized, paper based systems that are inefficient in terms of cost and public liability. To solve for these issues, e-Voting frameworks have been proposed in the literature, activating the use of electronic devices or systems to cast or count votes in an election. Despite being mostly centralized and suffer from single-point(s) of failure limitation, e-Voting still provides many advantages over traditional paper-based voting, such as higher efficiency, lower cost, and greater accessibility. Because of these advantages, many proposals and initiatives around the world have been announced motivating the adoption of e-Voting schemes to enhance the prosperity of the democratic process in their countries (e.g. Switzerland Kenya Sri Lanka Australia India Brazil Nigeria Russia among others. More sophisticated and reliable decentralized solutions typically use the Blockchain (BC) technology to achieve the required levels of decentralization, leading to public trust. BC is a revolutionary technology that allows for the creation and maintenance of a distributed ledger of transactions (TXs) that is secure, transparent, and immutable. This technol ogy

was first introduced by Satoshi Nakamoto in 2008, as the underlying technology for the bitcoin cryptocurrency. Since then, BC has been applied to various domains, such as Internet of Things (IoT) finance supply chain healthcare and Electronic Voting (e-Voting). BC technology offers a potential solution to some of the aforementioned challenges, by providing a decentralized and distributed platform for e-Voting that can enhance the trustworthiness and transparency of the voting process. BC-enabled e-Voting systems can store the votes in an immutable and tamper-proof way, and allow anyone to verify the validity and correctness of the votes. They can also protect the privacy and anonymity of the voters, by using cryptography techniques such as encryption, hashing, and zero-knowledge proofs. However, state-of-the-art solutions do not typically adhere to the most recommended privacy-by-design principles, and thus they are hardly adopted in realistic scenarios. BC-based e-Voting also faces many challenges, related to ensuring the security, integrity, privacy, and verifiability of the voting process and results. For instance, despite the technological advancements, current e-Voting systems often suffer from insufficient privacy measures, which can compromise the integrity of voter data and undermine trust in these systems. Moreover, scalability and performance issues are critical considerations particularly for deploying e-Voting systems across various network tiers, from small communities to large-scale elections. Additionally, BC-based e-Voting systems need to provide user-friendly interfaces and experience for the voters, who may not be familiar with the technical aspects of the system. Front-end DevOps teams are typically aware of the security and privacy threats related to their parts of the solution implementation. Yet, addressing privacy concerns in the back-end is directly related to the understanding of the BC technology as an enabler to e-Voting through several different approaches (e.g. Smart Contracts). The hardship in addressing privacy, security, and scalability needs by front-end, back-end, and system architects increases when developers are unaware of the complex methods used in BC. BC-based e-Voting systems must also comply with the legal and regulatory frameworks of different countries and regions, which may have different requirements and standards for e-Voting. For example, despite the mass adoption of BC technology in Europe, any application must adhere to the very strict General Data Protection Regulations (GDPR), aiming to protect the privacy of citizens in the

continent. Neglecting the GDPR-compliance requirement might lead to billions of Euros paid as fines against system developers.

II. RELATED WORK

A. Implementation of blockchain-based e-voting system

An electronic voting portal should provide security, integrity, vote transparency, and voter privacy. Electronic voting, or e-voting, has been used in many ways since the 1970s, with essential advantages over paper-based systems, such as higher efficiency and fewer errors. However, attaining widespread acceptance of such systems remains a problem, particularly in enhancing their resistance to potential mistakes. Blockchain is a cutting-edge technology that has the potential to improve the overall security of electronic voting systems. This paper uses smart contracts to develop an e-voting Decentralized Application (DApp) on the Ethereum blockchain and develops a frontend to access the DApp easily on the blockchain. This paper began with an overview of blockchain and explored the blockchain application challenges. One of the things that can be improved is the election voting system that leaves so many gaps for incompetence and tampering with the votes collected, as witnessed by so many real-life cases in our country. Finally, the added visibility of the voting procedure and more effective security can help in providing a fair result. This article also discussed using blockchain, essentially the smart contract function of the Ethereum blockchain, to make a decentralized app for the voting procedure of an election. It provides full transparency over the votes, with real-time tracking by using an election DApp. The blockchain makes it possible to have a fully transparent election while keeping all the voters anonymous.

B. ACB-vote:Efficient, f lexible, and privacy- preserving blockchain-based score voting with anonymously convertible ballots

Blockchain has emerged as a decentralized platform for e-voting. Among various blockchain-based voting systems, score voting provides flexible choices and better reflects public opinions. However, existing blockchain-based score voting systems suffer from heavy range proof overheads, and are much inefficient compared with other blockchain-based voting systems. Besides, voter anonymity in these systems is not rigorously addressed. In this paper, we

propose an efficient, flexible and privacy-preserving score voting system, named ACB-Vote, from anonymously convertible ballots. ACB-Vote achieves voting anonymity with BBS+ signature and signature of knowledge. Driven by convertibly linkable signatures (CLS), ACB-Vote allows cast ballots to be converted, where the conversion mechanism prevents anonymous voters from multiple voting. Besides, the proposed system avoids heavy range proofs, enables batch ballot verification and facilitates flexible tallying methods. We formally define a security model for ACB-Vote and provide rigorous security proofs. Experiments show that the efficiency of ACB-Vote is competitive compared with the previous score voting systems and is affordable in blockchain environments.

C. Trustful blockchain-based framework for privacy enabling voting in a university

In this study, we explore the challenges and potential solutions to blockchain-based voting. As a first step, we present a comparison of the relevant platforms for implementing smart contracts in decentralized applications (dApps). We analyze the top platforms, highlighting their advantages and disadvantages, their architecture, and which are more reliable for developing smart contracts. The goal is to find a technology that offers various facilities to the developer and multiple functionalities and performance in the development of smart contracts in a field that has seen an incredible pace of innovation. Based on the findings from our research, we propose a framework based on blockchain technology and smart contracts for university-level voting based on blockchains.

III. PROPOSED METHODOLOGY

The proposed system addresses these limitations by introducing smart contracts for transparent and reliable vote handling, differential privacy for enhanced voter anonymity, and Self-Sovereign Identity (SSI) for decentralized identity management using verifiable credentials. A novel (k, ε)-differential privacy algorithm is applied by using a pivot candidate strategy to anonymize votes through redistribution. To improve user interaction, a real-time notification system sends mobile alerts confirming successful voting. The implementation using Hyperledger DID's in a geographically distributed, cloud-based blockchain network demonstrates significant improvements in latency, accuracy, and privacy protection.

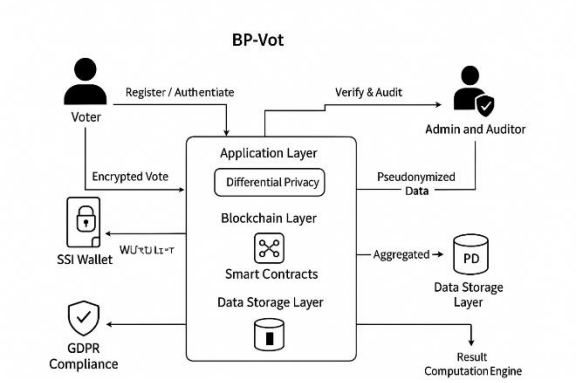
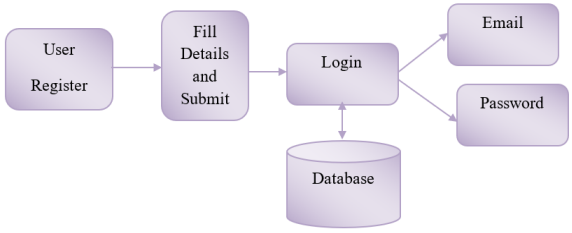


Fig. 1: System Overview

1. User Authentication Module

This module manages secure login for both voters and administrators. Passwords are hashed using SHA-256 or bcrypt before storage to prevent credential leaks. Role-based access ensures that voters and admins access only their respective dashboards. The system also tracks login attempts, supports session management, and may include CAPTCHA or OTP verification for enhanced security.

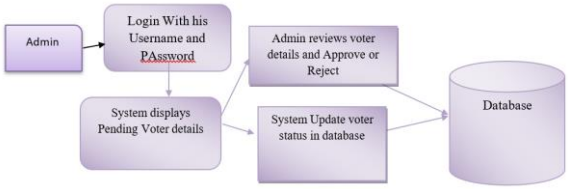


2. Voter Registration Module

Allows new users to register by providing identification details (name, email, voter ID, etc.). During registration, the system validates uniqueness of credentials and stores voter data in the database with encryption and consent records. Upon completion, a verification token is generated and sent for admin approval before activation.

3. Voter Verification Module

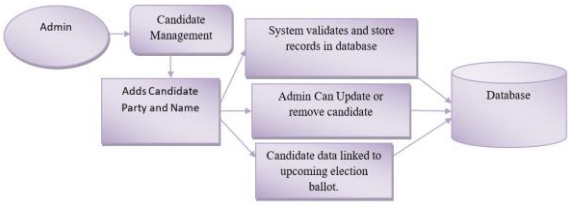
This module enables administrators to verify registered voters. The admin can review voter details, validate identity documents, and either approve or reject registrations. Approved voters receive activation emails and can then log in to cast votes. The verification ensures only legitimate and unique voters participate in the election.



4. Candidate Management Module

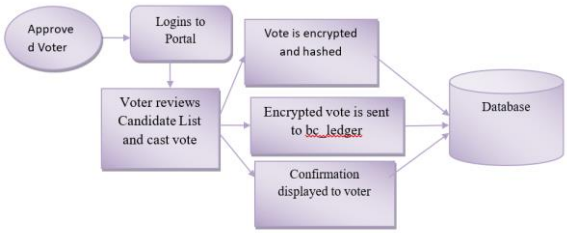
This module allows the administrator to add, update, or delete candidate profiles. Each candidate entry includes name, party, and manifesto information. The data is securely stored and later linked to ballots during

voting. Candidate information is displayed dynamically to voters on the voting page.



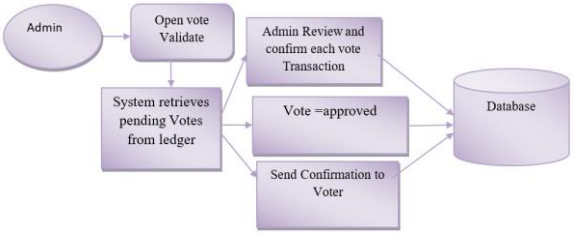
5. Voting Module

This is the core functional module where approved voters securely cast their votes. The system ensures one vote per voter using authentication and blockchain transaction linkage. Each vote is encrypted, digitally signed, and transmitted to the blockchain ledger through a smart contract interface to prevent tampering or duplication.



6. Vote Validation Module

After vote submission, the admin uses this module to validate and confirm recorded votes. The validation process includes checking digital signatures, timestamp verification, and ensuring integrity within the blockchain ledger. Invalid or duplicate votes are automatically rejected.



7. Result Visualization Module

Displays real-time election outcomes once voting concludes. The results are fetched from the blockchain ledger and represented using dynamic charts and tables (via Chart.js or Google Charts). Only verified votes are considered, and results are cryptographically verified for transparency.

8. Blockchain Vote Ledger Module

Acts as the backbone of the e-voting system. It records every verified vote as an immutable transaction on the blockchain ledger. Each block contains the vote hash, voter pseudonym, candidate ID, and timestamp. This ensures auditability, transparency, and tamper-proof storage of all voting activities.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the integration of Blockchain Technology and smart contracts ensured tamper-resistant vote recording and transparent vote verification throughout the election process. The email-based voter authentication mechanism achieved high verification accuracy while preventing unauthorized voting attempts.

The implementation of Differential Privacy effectively protected voter anonymity and prevented disclosure of individual voting preferences without affecting the correctness of election results. The analysis confirms that the proposed framework provides a secure, transparent, scalable, and privacy-preserving solution for modern electronic voting applications.

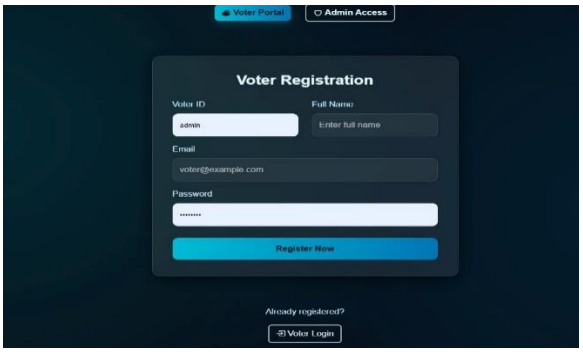


Fig. 2: Registration

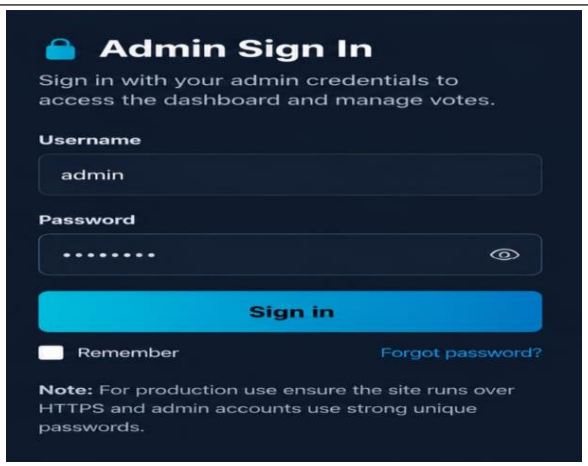


Fig. 3: Login

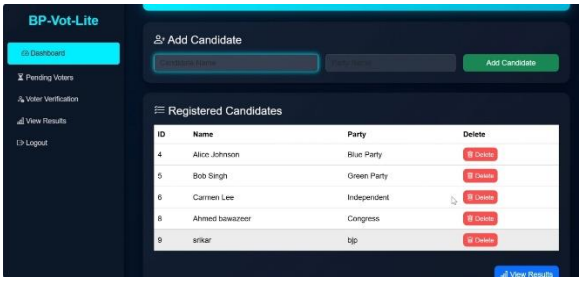


Fig. 4: Add Candidates

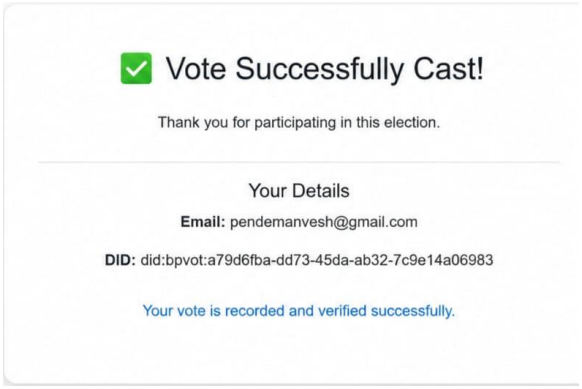


Fig. 5: Vote Successful

V. CONCLUSION

The proposed BP-Vot: Blockchain-based Privacy-Preserving e-Voting System successfully demonstrates a secure, decentralized, and transparent voting

mechanism that ensures voter anonymity and integrity of results. By integrating Blockchain technology, Smart Contracts, Differential Privacy, and Self-Sovereign Identity (SSI), the system effectively addresses critical challenges of traditional and centralized e-voting platforms, such as data tampering, identity leakage, and single points of failure. The implementation on a Hyperledger Besu blockchain network enhances trust and decentralization, providing tamper-proof and auditable election records. Experimental evaluations indicate that the system achieves up to 24% lower latency and maintains over 98% accuracy in vote aggregation even under varying conditions of candidate numbers and vote volume. The qualitative analysis confirms that BP-Vot ensures strong privacy protection as the number of votes increases, while maintaining system scalability and performance. Overall, BP-Vot represents a significant step forward in realizing a GDPR-compliant, privacy-preserving, and reliable decentralized e-voting solution suitable for real-world democratic applications.

REFERENCES

[1] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, ‘‘A review of E voting: The past, present and future,’’ Ann. Telecommun., vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.

[2] W. Bokslag and M. de Vries, ‘‘Evaluating e-voting: Theory and practice,’’ 2016, arXiv:1602.02509.

[3] M. Hapsara, ‘‘Reinstating e-voting as a socio-technical system: A critical review of the current development in developing countries,’’ in Proc. IEEE Region 10 Symp. (TENSYMP), May 2016, pp. 282–287.

[4] S. Risnanto, Y. B. A. Rahim, and N. Suryana, ‘‘Success implementation of E-voting technology in various countries: A review,’’ in Proc. FoITIC, Jan. 2020, pp. 150–155.

[5] L. E. Pleger and A. Mertes, ‘‘Use and assessment of E-voting systems: Findings from an online-survey among Swiss nationals living abroad,’’ Yearbook Swiss Administ. Sci., vol. 9, no. 1, p. 1, Sep. 2018.

[6] J. JumaandC.O.Oguk,‘‘Election results’ verification in e-voting systems in Kenya: A review,’’ Int. J. Social Sci. Inf. Technol., vol. 2020, pp. 1–14, Dec. 2020.

[7] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

[8] Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.

[9] Akinapalli, S. (2024). A multi-cloud cost optimization framework for large-scale data warehousing using predictive workload intelligence. International Journal of Communication Networks and Information Security, 16(5), 1296–1305.

AUTHORS Profile

Mrs. D. KRISHNA VENI has received her B.Tech from JNTUH, Hyderabad in 2011, M.Tech degree in Computer science from JNTUH, Hyderabad in 2021 and Pursuing Ph.D degree in Computer Science from Guru Naanak university, Ibrahimpatnam. She is dedicated to teaching field from the last 8 years. Her research area Machine Learning. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Ms. DAYALA VARSHITHA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. SAI LIKITHA BHIMANATHUNI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. PENDEM ANVESH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. MARAM REDDY SREEKAR REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.