International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 4 (April 2025), PP 158-160

Blockchain Based E-Voting in Electronic Elections

Dr. K N D Malleswararao[1]*, Shaik Sabeeha[1], Mokshith Sai Kola[1], Paturi Mohan Sai Krishna[1], and Tholusuri Shyam Akhil[1]
[1]*Department of IT,*
Dhanekula Institute of Engineering and Technology, AP, INDIA

ABSTRACT
The development of e-Government requires a secure, transparent, and efficient electronic voting (e-voting) system to increase electoral integrity and public confidence. Conventional e-voting systems suffer from ongoing security threats, transparent issues, and vulnerability to manipulation. Blockchain technology presents itself as a revolutionary solution to these threats by providing decentralized, immutable, and verifiable election processes. This paper introduces a new blockchain-based e-voting system that provides end-to-end security, transparency, and voter privacy. The platform is autonomous from a central authority, using cryptographic methods like homomorphic encryption to secure voter identities while ensuring data integrity. With extensive testing across various blockchain implementations-public and private blockchains-we show the practicability of our solution in real-world electoral contexts. Our findings show that blockchain-based e-voting not only prevents risks due to centralized control but also increases auditability and voter trust. This work adds to the development of secure electronic voting by combining blockchain's decentralized nature with privacy-preserving cryptographic techniques, making way for a more democratic and tamper-evident voting process.

Date of Submission: 05-04-2025 Date of acceptance: 15-04-2025

I. INTRODUCTION

The increasing popularity of e-Government initiatives further highlights the necessity of an effective and secure e-voting system [1, 2]. Nevertheless, the success of e-Government relies upon the digitalization of core public services like elections. According to different researchers, "E-voting is one of the key public sectors that can be transformed by blockchain technology" [3]. With the evolution of e-voting systems, there are newer challenges to be met that need to be resolved so that they can be viable. Electronic election security is one of the major issues, which needs to be as secure as the conventional paper-based voting system [4]. Electoral fraud, unauthorized use, and tampering with the votes are potential threats that require a system in which the voter has implicit faith [5]. With growing dependence on blockchain technology in protecting online transactions, it has become a promising solution for attesting to the integrity and transparency of the e-voting system [6]. Blockchain technology offers a decentralized method of conducting elections without dependency on a central system [7]. Centralized control in conventional voting systems risks issues of tampering and manipulation of election results. On the other hand, an e-voting system based on blockchain ensures the body in charge of conducting the elections cannot compromise the results [8]. Moreover, the transparency deficit in most of the current e-voting systems has created distrust on a large scale and decreased voter trust [9]. Blockchain technology eliminates this problem by providing total transparency and enabling all parties to view and audit election information in real-time [10]. This feature guarantees that votes are cast immutably, making any type of post-election changes or fraud impossible [11]. From a safety perspective, e-voting over blockchain is far better than using traditional electronic voting systems that fail to integrate the use of blockchain [12]. Using cryptographic methodologies like homomorphic encryption, one can ensure secrecy for the voter while still recording the integrity of the election [13]. More importantly, by being decentralized in nature, using blockchain makes cyberattacks much easier to resist and thus far tougher for hackers or malicious actors to infiltrate [14]. With these benefits in mind, our research aims to create a safe and clear e-voting system using blockchain technology.

II. MATERIAL AND METHODS

2.1 System Architecture

The blockchain e-voting system is structured in such a way that it can provide decentralization, transparency, security, and anonymity to voters. The system architecture consists of various necessary elements that collaborate in order to conduct a secure and efficient election.

2.2 Admin Tasks

The design of the blockchain e-voting system is systematic in nature for providing security, transparency, and efficiency. The process is initiated by admin operations, where the election administrator logs into the system (Fig. 1) through a secure authentication process. This allows only authorized staff to access the election parameters to be edited. The administrator is also in charge of inserting political parties(Fig. 2), candidates, and their respective symbols into the system, an important step through which the voters get to pick their choices easily. The system imposes stringent access control measures to avoid unauthorized changes, hence ensuring the integrity of the electoral process.

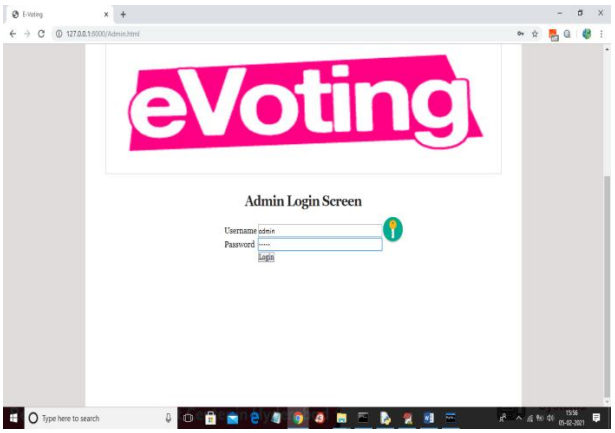

Fig 1. Admin Login Screen

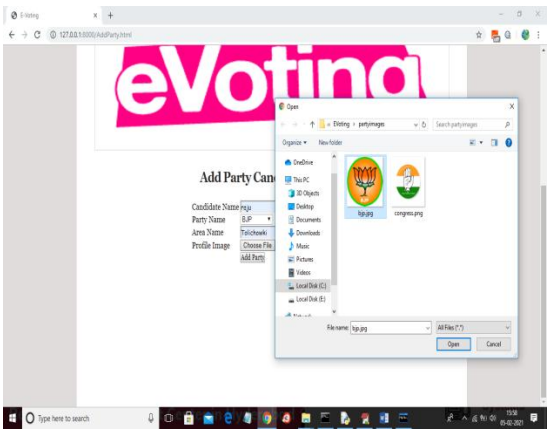

Fig 2. Adding Party and Candidate Details

2.3 Vote verification and transparency

The platform also features a strong vote verification and transparency (Fig. 3) tool. Each vote cast on the blockchain has a special transaction hash, with voting results being easily verifiable by approved auditors without divulging voters' anonymity. Because blockchain is a decentralized and distributed ledger, election information is available to all parties in an untamperable manner. This aspect greatly improves voter trust in the electoral process by averting vote tampering fears.

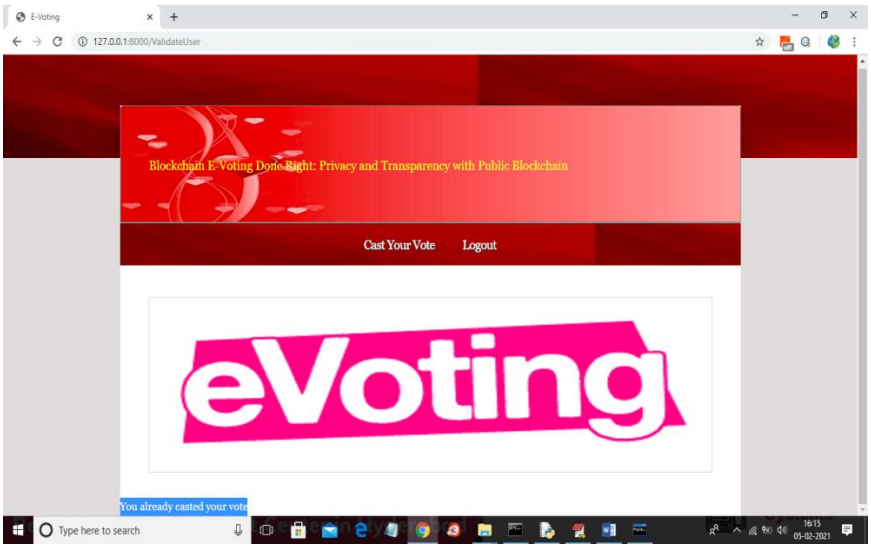

Fig 3. Duplicate Voting Attempt Message – 'You Already Casted Your Vote

III. RESULTS AND DISCUSSION

3.1 Vote Recording and Processing Speed

- The results indicate that Hyperledger Composer and Ganache significantly outperform Ethereum Ropsten in vote recording time and transaction processing speed.
- This is due to Ethereum's reliance on proof-of-work (PoW)**,** which involves mining delays and gas fees, leading to slower transaction confirmation times.
- In contrast, Hyperledger Composer and Ganache**,** which are private blockchain implementations, have faster consensus mechanisms, reducing latency in vote registration and processing.

3.2 Security Considerations

- Ethereum Ropsten offers the highest level of security due to its decentralized and public nature, making it less susceptible to manipulation**.**
- However**,** Hyperledger Composer and Ganache, being private blockchains, have better control over access but are more vulnerable to centralization risks.
- The integration of homomorphic encryption and zero-knowledge proofs ensures that even in a private blockchain, voter privacy and integrity of the election process are maintained.

3.3 Scalability and Resource Efficiency

- Ethereum's slow transaction speed and high gas fee**s** make it less scalable for national-level elections.
- Hyperledger Composer and Ganache, being permissioned networks, allow for more transactions per second with lower computational costs, making them ideal for enterprise and government-adopted voting systems**.**

IV. CONCLUSION

Comparing public and private blockchains for e-voting, both have distinctive benefits and compromises. Public blockchains like Ethereum Ropsten offer unparalleled transparency with the ability to monitor in real time, guaranteeing trust and auditability. Their lower transaction rates and higher computation fees, however, can limit scalability. Conversely, private blockchains such as Hyperledger Composer and Ganache provide faster processing times with average vote recording times of 6.32s and 6.05s, respectively, as opposed to Ethereum Ropsten's 17.75s. Private blockchains, while they are efficient, impose a level of centralization that restrict their openness and diminish total system credibility. Although network time differences are small, the openness of public blockchains makes them better for electoral systems, as data is kept open and verifiable.

REFERENCES

[1]. Alharbi, A., & Hussain, F. (2020). Blockchain-Based E-Voting: A Systematic Review.
[2]. Neff, C. A. (2001). A Verifiable Secret Shuffle and its Application to E-Voting.
[3]. Zhao, Z., & Li, Y. (2017). Secure Electronic Voting System Based on Blockchain Technology.
[4]. David, B., & Olivier, P. (2013). Zero-Knowledge Proofs and Applications.
[5]. Gritzalis, D. (2002). Secure Electronic Voting.
[6]. Benaloh, J. (2006). Simple Verifiable Elections.
[7]. Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.
[8]. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems.
[9]. Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document.
[10]. Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, L. (2014). Secure Multiparty Computations on Bitcoin.
[11]. Garay, J., Kiayias, A., & Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications.
[12]. Ryu, S. I., & Hong, S. (2021). Transparent and Decentralized E-Voting System Based on Blockchain.
[13]. Neff, C. A. (2001). A Verifiable Secret Shuffle and its Application to E-Voting.
[14]. Zhao, Z., & Li, Y. (2017). Secure Electronic Voting System Based on Blockchain Technology.