SecureVote: Enhancing Electoral Integrity Using Blockchain-Based E-Voting

Rhythm Garg
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India

Aashish Gupta
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India

Arti Sharma
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India

***Abstract*— Electronic voting (e-voting) has clear advantages over traditional paper-based systems, such as improved efficiency and reduced errors. However, gaining widespread public trust in e-voting systems remains a significant challenge, particularly in addressing their potential vulnerabilities. Blockchain technology has emerged as a promising solution to enhance the security and reliability of e-voting systems. This project explores how blockchain's transparency and cryptographic capabilities can create a secure, efficient, and user-friendly e-voting infrastructure. Using the Multichain platform, it aims to design and implement an e-voting mechanism that meets critical requirements like legality, accuracy, and security. Despite these advancements, digital voting still faces obstacles that may limit its acceptance. Blockchain's decentralised nature and end-to-end verification provide a strong foundation for tackling these issues, offering a pathway to more trustworthy and robust electronic voting systems.**

Keywords—E-Voting, Blockchain, Efficiency, Security, Decentralized.

I. INTRODUCTION

In any democracy, ensuring election security is vital to national security. Over the past decade, computer security experts have closely examined the potential of electronic voting systems to reduce election costs while enhancing security measures. Traditionally, democratic elections have relied on pen-and-paper voting methods. However, upgrading to modern election technology is essential for reducing fraud and enabling a traceable and verifiable voting process. [1]

II. IMPORTANCE OF BLOCKCHAIN

Information fuels business success, especially when it is timely and precise. Blockchain technology is uniquely suited to support this, offering real-time, accessible, and fully transparent data that are recorded on an unchangeable ledger—visible only to authorized users within the network. A blockchain network can monitor a wide range of activities, such as transactions, inventory, and sales. With everyone having access to the same verified data, users can view every aspect of a transaction from beginning to end, fostering trust and unlocking new possibilities.

A. Preventing Fraud and Cyber-attacks with Blockchain:

Blockchain technology addresses two significant online risks: double spending and data hacking. By requiring miner nodes to complete complex tasks (or "mining") to validate each transaction, blockchains prevent these issues. Unlike centralised databases that are vulnerable to breaches, blockchain's decentralised consensus mechanism safeguards data, making it nearly impossible for hackers to tamper with.

B. Essential Blockchain Tools and Consensus Mechanisms:

Blockchain technology is underpinned by various tools and consensus protocols that secure and verify transactions. Here are a few key elements:

1) Tools

- Wallets: Blockchain wallets are digital storage solutions that allow users to send, receive, and manage cryptocurrencies and other digital assets.
- Nodes: Nodes are individual computers that participate in verifying and validating transactions across the blockchain.

2) Blockchain Explorers:

- These tools enable users to view and trace transactions within the blockchain. Languages like Solidity are commonly used for creating smart contracts on Ethereum, though other blockchains may use unique programming languages for their contracts.

3) Consensus Mechanisms:

- Proof of Work: The original consensus model used by Bitcoin, in which miners compete to solve complex puzzles to validate transactions and add blocks.
- Proof of Stake: In PoS, validators are chosen based on the amount they "stake" in the network, making them eligible to confirm transactions.
- Byzantine Fault Tolerance: A robust consensus model designed to handle malicious actors in a decentralised network, often used in private blockchains.

The tools and consensus algorithms used in blockchain vary by platform and application, and as blockchain technology advances, we can expect even more innovative approaches to emerge.[9]

III. ELECTRONIC VOTING REQUIREMENTS:

The core specifications for an electronic voting system were outlined, and the proposed solution aligns with each requirement, ensuring a secure and reliable process. Below is an overview of the key criteria and how the system addresses them:

A. *Ensuring Voter Privacy:*

Maintaining the confidentiality of each voter's choice is paramount. The proposed solution leverages blockchain technology's cryptographic capabilities to safeguard voter privacy. When a voter registers, the system generates a unique voter hash that serves as their identifier within the blockchain network. Thanks to the collision-resistant nature of cryptographic hashing, this identifier cannot be exploited or traced back to the voter. This ensures that votes remain anonymous and secure, especially in situations where voter confidentiality could be at risk.

B. *Preventing Unauthorized or Duplicate Voting:*

The system ensures that only registered voters can participate and restricts each individual to a single vote. To achieve this, voters must register using official documents and special IDs, which are verified through a robust multi-layered approach. This process, combined with biometric authentication methods like fingerprint scanning, not only confirms voter eligibility but also eliminates the possibility of duplicate voting, thereby upholding the integrity of the election.[3]

The proposed e-voting system effectively meets two critical requirements: protecting voter anonymity with blockchain cryptography and ensuring voting legitimacy through advanced identification and authentication mechanisms. These measures work together to create a fair, secure, and trustworthy voting process.[2]

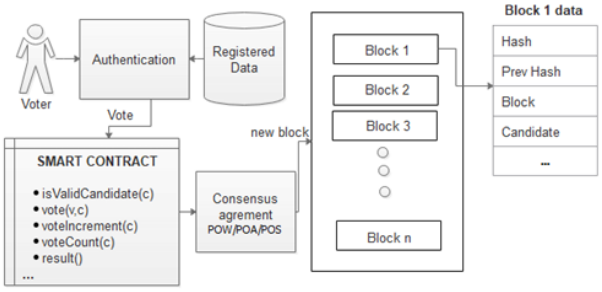

Fig. 1. Workflow of a basic blockchain-based e-voting system.

TABLE I. BLOCKCHAIN TYPES FOR DIFFERENT USE CASES.

Property	Public	Private	Consortium
Management	Decentralised	Organisation Controlled	Multiple Organisations
Consensus Determination	All miners	Organisation participating	Selected Miners
Participation	Permissionless	Permissioned	Permissioned
Immutability	Almost impossible to tamper	Controlled, could be tampered with.	It could be tampered with.
Transaction Duration	Longer	Short	Shortest
Efficiency	Low	High	High

IV. EXISTING E-VOTING SOLUTIONS

A. *Follow My Vote:*

This company offers a cutting-edge online voting platform built on blockchain technology, designed to provide unparalleled security and transparency. A unique polling box audit feature allows stakeholders to monitor real-time democratic progress. Voters can confidently cast their votes remotely, assured of safety and precision. The system leverages voter identification to unlock the virtual ballot box, locate their vote, and verify its accuracy. Moreover, it ensures that the election outcomes are mathematically validated, leaving no room for doubt about the integrity of the process.

B. *Agora*

This group pioneered a blockchain-based digital voting platform, established in 2015, and made waves by partially implementing it during Sierra Leone's presidential election in March 2018. Agora's innovative architecture integrates a custom blockchain, participatory security protocols, and a robust consensus mechanism to ensure reliability and trust. At the heart of Agora's ecosystem is the native token, aptly named "Vote," which incentivises citizens and authorised electoral bodies worldwide to champion a secure and transparent voting process. Serving as a universal token within the ecosystem, "Vote" reinforces Agora's mission of revolutionising elections on a global scale.

C. *Polys*

Polys is an advanced blockchain-powered online voting platform fortified by transparent cryptographic algorithms and backed by the expertise of Kaspersky Lab. Designed to cater to diverse communities, Polys enables student councils, unions, and associations to effortlessly organise polls while effectively disseminating electoral information to their members. By streamlining online elections, Polys fosters productivity within communities, strengthens connections between leaders and their groups, and draws in fresh supporters. Beyond enhancing engagement, Polys aims to save time and resources for local authorities, state governments, and other organisations, allowing them to prioritise meaningful tasks like collecting and refining proposals.

D. *Voat*

This company established a smartphone-based voting system on blockchain to vote remotely and anonymously and verify that the vote was counted correctly [70]. Voters confirm their applicants and themselves on the application and give proof by an image and their identification, including biometric confirmation that either a distinctive signature such as fingerprints or retinal scans.

V. LIMITATIONS IN THE EXISTING SYSTEM:

The realm of electronic voting systems faces significant challenges and limitations that must be addressed to ensure their effectiveness and acceptance:

A. *Accurate Voter Registration and Data Privacy:*

One major technical challenge is ensuring that all eligible voters are correctly registered and their data is in a format suitable for digital processing. Safeguarding personal identifying information is equally critical to maintain confidentiality and protect voter privacy.

B. *Casting Anonymous Votes:*

Maintaining voter anonymity during and after the voting process is paramount. Once submitted, each vote must remain private, inaccessible even to system administrators. This ensures both the confidentiality and integrity of the electoral process.

C. *Representing Votes Securely:*

Determining the best method for representing votes in online systems remains a topic of debate. Clear text communication risks compromising anonymity and integrity, while hashed tokens offer a potential solution. However, linking tokens to voters without compromising anonymity poses a complex challenge.

D. *Voter Verifiability:*

Voters should be able to review and verify their ballots during submission. This feature builds confidence in the voting system and serves as a safeguard against potential manipulation or errors.

E. *High Initial Setup Costs:*

Although electronic voting systems may be cost-efficient in the long term, their initial deployment can be prohibitively expensive, particularly for smaller organisations or enterprises.

F. *Rising Security Concerns:*

Cybersecurity threats, such as DDoS attacks and hacking, pose serious risks to the integrity of public elections. Protecting against tampering, ensuring data integrity, and maintaining transparency while safeguarding privacy are essential.

G. *Lack of Public Trust and Transparency:*

Winning public trust in the outcomes of digital elections can be difficult. Establishing a perception of transparency and reliability in a fully digital process is a major challenge that electronic voting systems must overcome.

H. *Remote Voting Delays and Inefficiencies:*

Remote voting relies heavily on stable, high-performance technology and infrastructure to ensure synchronous participation. Any inefficiencies or delays in this setup can undermine the process and voter trust.

Addressing these challenges is essential for electronic voting systems to be widely adopted, ensuring both their technical reliability and public confidence. [4][5]

VI. Objectives And the Problem:

This project aims to harness blockchain technology to overcome the current challenges of electronic voting systems. The primary objectives are:

1. Integrating a secure digital identity management system to verify voters.
2. Ensuring anonymity in the voting process while maintaining fairness.
3. Designing custom procedures to prevent tampering and ensure vote accuracy.
4. Establishing independently verifiable mechanisms for voter confidence.
5. Exploring cost-effective deployment strategies to reduce initial implementation expenses.
6. Enhancing cybersecurity measures to mitigate threats such as DDoS attacks and hacking.
7. Ensuring transparency and trust in the voting process using blockchain's immutable ledger.
8. Optimizing remote voting systems to improve efficiency and reduce delays.[8]

VII. Overcoming These Challenges:

To address the outlined obstacles, the system incorporates blockchain's strengths, such as transparency and immutability. Key approaches include:

1. Making the voting process verifiable and publicly auditable to inspire trust in the results.
2. Implementing mechanisms that ensure every vote is recorded accurately without duplication or tampering.
3. Using biometric and cryptographic methods to validate voter identities and prevent unauthorised access.
4. Structuring the system to neutralise undue influence from external entities.
5. Ensuring votes recorded on the blockchain are tamper-proof, protecting their integrity.
6. Allowing voters to confirm their votes without exposing their choices.

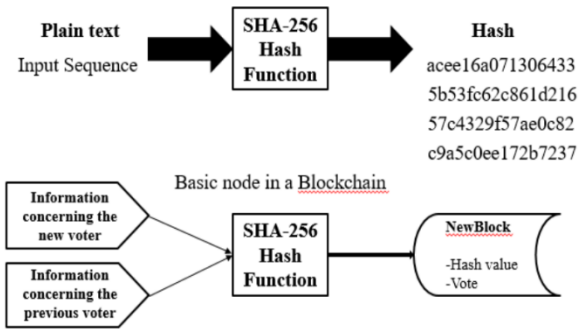

Fig. 2. SHA-256 working in blockchain.

VIII. Framework for the Proposed System:

The proposed e-voting framework draws inspiration from the Prêt à Voter system, ensuring essential features like privacy, eligibility, receipt-freeness, and verifiability. Key elements include:

1. A user-friendly web-based interface for seamless voting.
2. Cryptographic hashes for vote verification while maintaining voter anonymity.
3. Biometric-based mechanisms to prevent duplicate voting.
4. Administrative tools for efficient management of voters, constituencies, and candidates.

5. Voter confirmation via email containing transaction IDs, ensuring transparency and confidence in the system.[6][7][10]

IX. Conclusion:

This research paper aims to explore and assess critical aspects of electronic voting systems (EVS) built on blockchain technology. It delves into recent advancements in blockchain-based electronic voting (EV), beginning with an overview of blockchain principles and their applications.

Subsequently, the paper analyses current electronic voting methods, acknowledges their shortcomings and suggests potential solutions. Highlighting the significant potential of blockchain to revolutionise electronic voting, it reviews existing blockchain-based EV solutions and identifies emerging research opportunities in this field. Experts widely regard blockchain as a suitable foundation for decentralised electronic voting systems (EVS).

In modern society, the use of digital voting technologies presents an attractive opportunity to make public voting more cost-effective, efficient, and accessible. Additionally, it facilitates a more direct form of democracy, empowering individuals to voice their opinions on specific laws and initiatives.

References

[1] Mayuri Gomte, Harshal Chaudhari, Abhishek Tapare, and Dr. Y. M. Patil. (2023, April 28). "IoT-Based E-Voting System to Prevent Fraudulent Voting." International Journal of Advanced Research in Science, Communication and Technology, 289–293. https://doi.org/10.48175/ijarsct-9576

[2] Benny, A. (2020, August 11). "Blockchain-Based E-Voting System." *Blockchain Based E-voting System by Albin Benny: SSRN.* https://doi.org/10.2139/ssrn.3648870

[3] Taherdoost, H. (2023, February 13). "Smart Contracts in Blockchain Technology: A Critical Review." MDPI. https://doi.org/10.3390/info14020117

[4] Javaid, M. A. (2014). "Electronic Voting System Security." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2393158

[5] Khan, I., and Shahaab, A. (2021, February 2). "A Peer-To-Peer Publication Model on Blockchain." *Frontiers in Blockchain*, 4. https://doi.org/10.3389/fbloc.2021.615726

[6] "Smart Voting Platform (Secured Digital Voting System) Utilizing Blockchain Technology and Biometric Authentication." (2023, May 17). *International Journal of Science and Engineering Applications*, 105–113. https://doi.org/10.7753/ijsea1205.1029

[7] "Decentralized Online Voting System." (2023, May 31). *International Research Journal of Modernization in Engineering Technology and Science.* https://doi.org/10.56726/irjmets40446

[8] Virani, H., and Kyada, M. (2022, December 9). "A Systematic Literature Review on Smart Contracts Security." *arXiv.org.* https://arxiv.org/abs/2212.05099v1

[9] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., and Bani-Hani, A. (2021, April 18). "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." *PubMed Central (PMC).* https://doi.org/10.1007/s12083-021-01127-0

[10] Yao, J., Wei, L., and Liu, T. (2020, July 6). "Blockchain-Based Voting System." *Computer System Networking and Telecommunications*, 3(1). https://doi.org/10.18063/csnt.v3i1.1146

[11] "Blockchain Technology-Based E-Voting System" by Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, and Prathmesh Potdar. (*ITM Web of Conferences*, 32, 03001 (2020))