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

Rhythm Garg1   
*Dept. of Computer Science, KIET Group of Institutions, Ghaziabad, India*

Arti Sharma2  
*Dept. of Computer Science, KIET Group of Institutions, Ghaziabad, India*

ABSTRACT*:* Electronic voting has clear advantages over traditional systems, such as improved efficiency and reduced errors. But gaining widespread public trust in e-voting systems still 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 looks into how blockchain’s transparency can make e-voting more secure, efficient, and easy to use. The aim is to create a voting system that checks all the important boxes like being legal, accurate, and secure.

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

# Introduction

In any democracy, keeping elections secure is crucial for protecting national security. Over the last decade, computer security experts have been exploring how electronic voting systems could lower election costs while boosting security. While pen-and-paper voting has been the go-to method for democratic elections, switching to modern technology can help reduce fraud and create a voting process that's both traceable and verifiable. [1]

# Importance of Blockchain

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

1. *Preventing Fraud and Cyber-attacks with Blockchain:*

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

1. *Essential Blockchain Tools and Consensus Mechanisms:*

Blockchain technology relies on various tools and consensus protocols to ensure secure and verified transactions. Here’s a quick breakdown of the key elements:

1. Tools:
2. Wallets: Digital wallets let users send, receive, and manage cryptocurrencies and other digital assets securely.
3. Nodes: These are individual computers that play a crucial role in verifying and validating transactions on the blockchain network.
4. Blockchain Explorers: These tools let users track and view transactions happening on the blockchain. For example, Solidity is a popular programming language for creating smart contracts on Ethereum. Other blockchains may use their own specialized languages for smart contract development.
5. Consensus Mechanisms:
6. Proof of Work: The original consensus model used by Bitcoin, in which miners compete to solve complex puzzles to validate transactions and add blocks.
7. Proof of Stake: In PoS, validators are chosen based on the amount they "stake" in the network, making them eligible to confirm transactions.
8. Byzantine Fault Tolerance: A robust consensus model that handles malicious actors in a decentralised network, often used in private blockchains.[9]

# 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:

1. 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 voters register, the system generates a unique voter hash 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 when voter confidentiality is at risk.

2. 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 unique IDs, 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 meets two critical requirements: protecting voter anonymity with blockchain cryptography and ensuring voting legitimacy through advanced identification and authentication mechanisms. These measures create a fair, secure, and trustworthy voting process.[2]

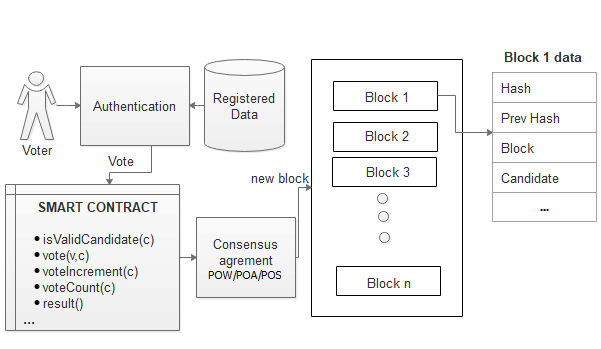


Fig. 1: Workflow of a basic blockchain-based e-voting system.

# Existing E-Voting Solutions

1. 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.

1. 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.

1. 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 community productivity, 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.

# 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:

1. 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.

2. Casting Anonymous Votes: Maintaining voter anonymity during and after voting 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.

3. 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.

4. Voter Verifiability: Voters should be able to review and verify their ballots during submission. This feature builds confidence in the voting system and safeguards against potential manipulation or errors.

5. 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.

6. 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.

7. Lack of Public Trust and Transparency: Winning public trust in the outcomes of digital elections can be problematic. Establishing a perception of transparency and reliability in a wholly digital process is a significant challenge that electronic voting systems must overcome.

8. 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]

# 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. Custom procedures are designed to prevent tampering and ensure vote accuracy.
4. Establishing independently verifiable mechanisms for voter confidence.8]

# OVERCOMING THESE CHALLENGES

The system incorporates blockchain’s strengths, such as transparency and immutability, to address the outlined obstacles. 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.

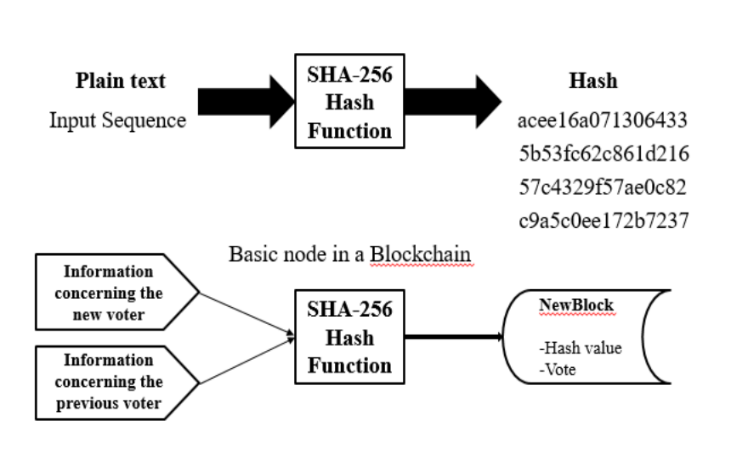


Fig. 2: SHA-256 working in blockchain.

# 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 efficiently managing voters, constituencies, and candidates.

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

# 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, digital voting technologies present an attractive opportunity to make public voting more cost-effective, efficient, and accessible. Additionally, they facilitate 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)).

[12] The Benefits of White Label Crypto Wallets | Light e Luz. <https://lighteluz.com/the-benefits-of-white-label-crypto-wallets/>

[13] Permissionless Blockchain: An Overview. <https://www.solulab.com/understanding-permissionless-blockchain/>

[14] The Rise Of Micro-credentials And Digital Badges — The Education Daily. <https://theeducationdaily.com/micro-credentials-and-digital-badges/>