A SECURE BLOCKCHAIN BASED VOTING SYSTEM

Sagar.K.R,Kavya.T.M,Komala.G.R,Likhitha.G,Shambhavi.R

[1] Sagar K R Asst prof ,Computer Science and Engineering,SJM Institute of Technology,Karnataka,India
[2] Kavya T M Student,Computer Science and Engineering,SJM Institute of Technology,Karnataka,India
[3] Komala G R Student,Computer Science and Engineering,SJM Institute of Technology,Karnataka,India
[4] Likhitha G Student,Computer Science and Engineering,SJM Institute of Technology,Karnataka,India
[5] Shambhavi R Student,Computer Science and Engineering,SJM Institute of Technology,Karnataka,India

ABSTRACT

In a rapidly digitizing world, our democracy must evolve alongside technology. This project marks a revolutionary leap in electoral innovation—a Blockchain-Based Voting System designed to transform how nations vote, protect, and prosper. Gone are the days of ballot boxes, rigged elections, and cyber vulnerabilities. Every vote in this system is not just cast—it's encrypted, hashed, secured, and permanently stored on the blockchain. Leveraging military-grade AES encryption, each vote becomes an impenetrable digital vault, while SHA-256 hashing ensures data integrity. The blockchain then seals it all within an unbreakable, transparent chain that guarantees every vote remains authentic and untampered. Only the true voice of the people, visible and verifiable by all. This platform eliminates threats like vote tampering, identity fraud, and cyberattacks, redefining trust in the electoral process. By combining hyper-security with radical transparency, it doesn't just improve elections—it reinvents them. This is more than a project, it's a movement toward fearless, corruption-free, and uncompromised democracy. The future of free and fair elections is here—and it's built on blockchain.

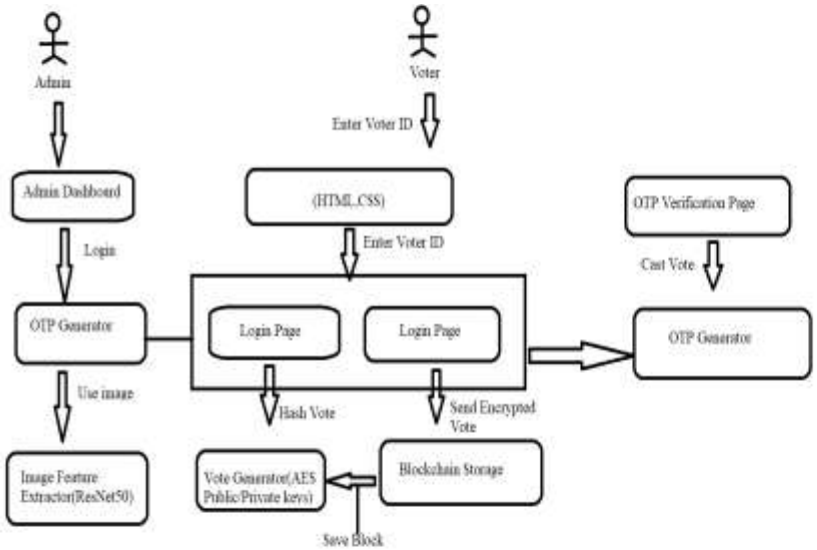
Keyword *Digital democracy,AES Encryption,SHA-256 Hashing,Data Integrity,Transparent Eelctions*

1. INTRODUCTION

The Blockchain-Based Voting System offers a modern, secure, and transparent solution to the growing challenges faced by traditional electoral processes. As concerns such as voter impersonation, ballot tampering, duplicate voting, and result manipulation continue to undermine public trust, this system leverages blockchain's immutable distributed ledger to ensure that every vote is recorded as a permanent, tamper-proof entry. Advanced cryptographic techniques protect voter privacy, while strong authentication methods—such as multi-factor verification and biometric identification—guarantee that only legitimate voters can participate. Additionally, the system enables real-time auditing and transparent result validation without compromising anonymity, allowing stakeholders to monitor every stage of the election process. By integrating decentralization, strong encryption, and robust identity verification, the Blockchain-Based Voting System provides a reliable and future-ready framework that enhances electoral security, efficiency, and public confidence in democratic participation.

2. METHODOLOGY

The methodology of the Blockchain-Based Voting System involves a structured and secure process that ensures transparency, integrity, and trust throughout the election. The system begins with the initialization of a blockchain network where election authorities configure cryptographic keys, network parameters, and upload verified voter records. During the voting phase, each voter undergoes a strict authentication procedure using multi-factor verification methods such as OTP checks, government ID validation, and biometric identification to ensure that only legitimate participants can cast a vote. Once authenticated, the voter submits their choice, which is immediately encrypted using advanced algorithms like AES to guarantee privacy. The encrypted vote is then hashed using SHA-256 to maintain data integrity before being broadcasted to the blockchain network. Participating nodes validate the vote through a consensus mechanism and store it permanently as a tamper-proof entry in the blockchain. This decentralized and immutable storage eliminates risks of manipulation or cyberattacks. Throughout the process, stakeholders can monitor and audit voting activities in real time without compromising voter anonymity. Vote counting is carried out securely either through on-chain smart contracts or by authorized officials using controlled decryption keys, ensuring the tallied results are accurate and verifiable. Finally, the validated results are published transparently, and the blockchain ledger is archived for future audits, providing a reliable and future-ready methodology for conducting free and fair elections.

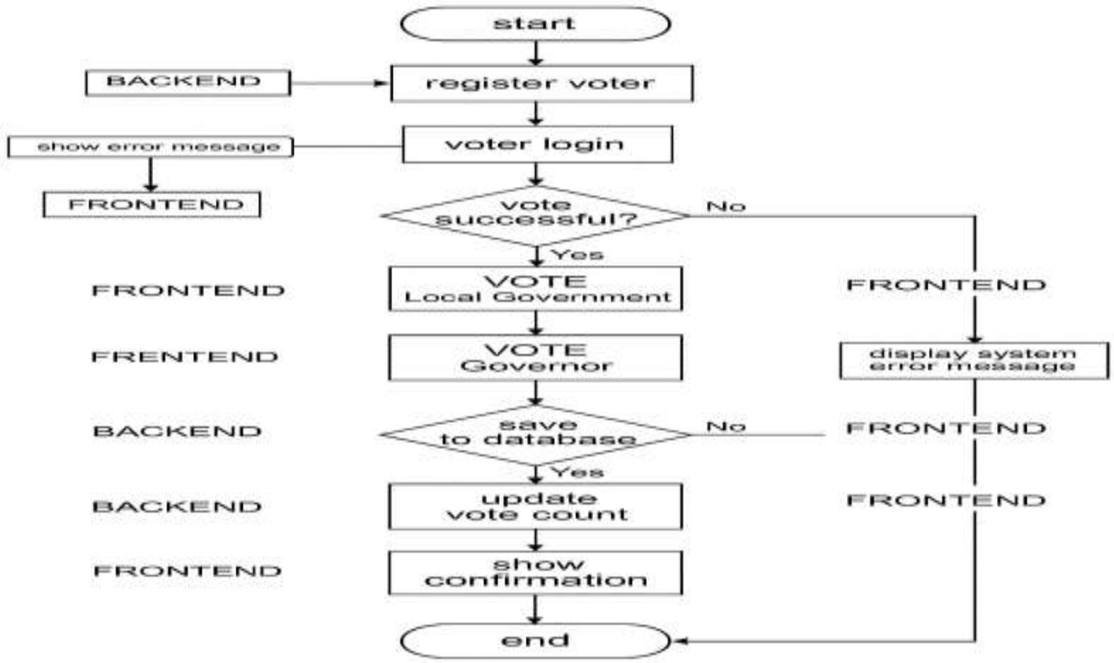


Architecture

2.1 Working Principle

The working principle of the Blockchain-Based Voting System is grounded in cryptographic protection, decentralized architecture, and consensus-based validation. The process begins when a voter enters the system and passes through a strong authentication mechanism—such as OTP verification, biometric matching, or government ID validation—to confirm their identity. Once authenticated, the voter’s choice is encrypted using advanced cryptographic algorithms to ensure complete privacy. This encrypted vote is then converted into a unique hash value that acts as a digital fingerprint, guaranteeing that no one can alter or manipulate the vote without detection. The encrypted and hashed vote is broadcast to the blockchain network, where multiple independent nodes verify its authenticity through a consensus mechanism. This distributed validation ensures that only legitimate, properly authenticated votes are accepted.

After validation, the vote is added to a new block along with other verified votes, and this block is cryptographically linked to the previous one, forming an immutable and tamper-proof chain. The decentralized nature of the blockchain ensures that the ledger is stored across multiple nodes, preventing any single entity from modifying or controlling the data. Even if one node is compromised, the network as a whole remains secure due to redundancy and cross-verification among nodes. Throughout the entire process, stakeholders can monitor entries on the blockchain in real time without accessing voters’ identities, maintaining both transparency and anonymity. Since each vote is permanently recorded and cannot be altered, deleted, or duplicated, the system guarantees high levels of trust, integrity, and accountability, providing a secure and transparent framework for conducting modern digital elections.



Flow chart

3 Software and Hardware Requirements

Software Requirements

- Windows/Linux
- Fabric
- MySQL/XAMPP
- Python
- HTML/CSS
- AES or SHA-256

In our Secure Blockchain-Based Voting System project, Windows or Linux serves as the primary operating environment for running development tools, blockchain nodes, and backend services, with Linux offering enhanced stability for Fabric deployment. Hyperledger Fabric acts as the core blockchain framework, enabling a permissioned and tamper-proof voting process where smart contracts record and validate each encrypted vote. For managing non-sensitive voter data such as login credentials and system logs, we use MySQL/XAMPP, which provides a reliable backend database environment. Python plays a crucial role in implementing backend logic, handling cryptographic operations, managing APIs, and securely connecting the frontend to the blockchain network. The user interface is developed using HTML and CSS to ensure a simple, responsive, and user-friendly voting experience. To secure voting data, AES encryption is used to encrypt each vote, and SHA-256 hashing is applied to maintain data integrity before storing the vote on the blockchain. Together, these components create a secure, transparent, and efficient digital voting system that preserves privacy, prevents tampering, and strengthens the overall electoral process.

Hardware Requirements

- Multi-core CPU(Quad-core or Higher,2.5 GHz+)
- Minimum 16GB RAM for Blockchain nodes
- Encrypted SSD(256GB-1TB Storage)
- Smartphone or PC with stable internet and modern browser

The secure blockchain-based voting system requires a robust hardware setup to ensure smooth performance, efficient processing, and high security. A multi-core CPU, preferably a quad-core processor or higher with speeds above 2.5 GHz, is essential for handling blockchain operations, validating transactions, and running multiple system services simultaneously. To support the resource-intensive nature of blockchain nodes, a minimum of 16 GB RAM is recommended for stable operation and faster block processing. An encrypted SSD ranging from 256 GB to 1 TB provides the necessary storage capacity for blockchain data, system logs, and cryptographic files while ensuring secure and fast read/write operations. For end-users, the system supports voting through a smartphone or PC as long as the device has a stable internet connection and a modern web browser, ensuring accessibility and ease of use for all voters. This combination of strong server hardware and accessible client-side devices helps maintain security, reliability, and efficiency throughout the voting process.

4. CONCLUSION

The concept of integrating online voting systems to make public elections cheaper, faster, and more convenient is highly relevant in modern society. By reducing cost and time, online voting can help normalize the electoral process, minimize barriers between voters and elected officials, and increase accountability. It also enables a more transparent and participatory form of democracy where citizens can directly express their views on specific bills and initiatives. In this project, we implemented a blockchain based online voting framework that uses smart contracts to ensure secure, reliable, and cost-effective elections while maintaining voter privacy. Compared to earlier methods, our approach demonstrates that blockchain technology provides a promising opportunity for democratic nations to transition from traditional paper-based voting and electronic voting machines to a more efficient and secure system. This enhances overall security, reduces operational costs, and improves accessibility for voters.

5. REFERENCES

1. **Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.**
   – Provides foundational concepts of blockchain relevant for secure voting applications.
2. **Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." *IEEE International Congress on Big Data*.**
   – Explains core mechanisms like blocks, hashing, and consensus essential for e-voting security.
3. **Noizat, P. (2015). "Blockchain Electronic Vote." In *Handbook of Digital Currency* (pp. 453–461). Elsevier.**
   – Discusses use of blockchain specifically for voting systems.
4. **Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). "Opportunities and Risks of Blockchain Technologies in Business." *IEEE Software*, 34(1), 20–25.**
   – Covers blockchain risks and opportunities for secure implementation.
5. **McCorry, P., Shahandashti, S. F., & Hao, F. (2017). "A Smart Contract for Boardroom Voting with Maximum Voter Privacy." *International Conference on Financial Cryptography and Data Security*.**
   – Introduces privacy-preserving smart contract-based voting.
6. **Kshetri, N., & Voas, J. (2018). "Blockchain-Enabled E-Voting." *IEEE Software*, 35(4), 95–99.**
   – Discusses how blockchain can improve transparency and reduce fraud in elections.
7. **Hjalmarsson, F., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). "Blockchain-Based E-Voting System." *IEEE Cloud Computing*, 5(1), 18–24.**
   – Presents architecture of a blockchain voting platform.