Blockchain-Based Secure Voting System

Project by:
1. Mohammed Anas - 22R21A05N8
2. T. Varshith Reddy - 22R21A05R0
3. D. Bharath Kumar - 22R21A05M4

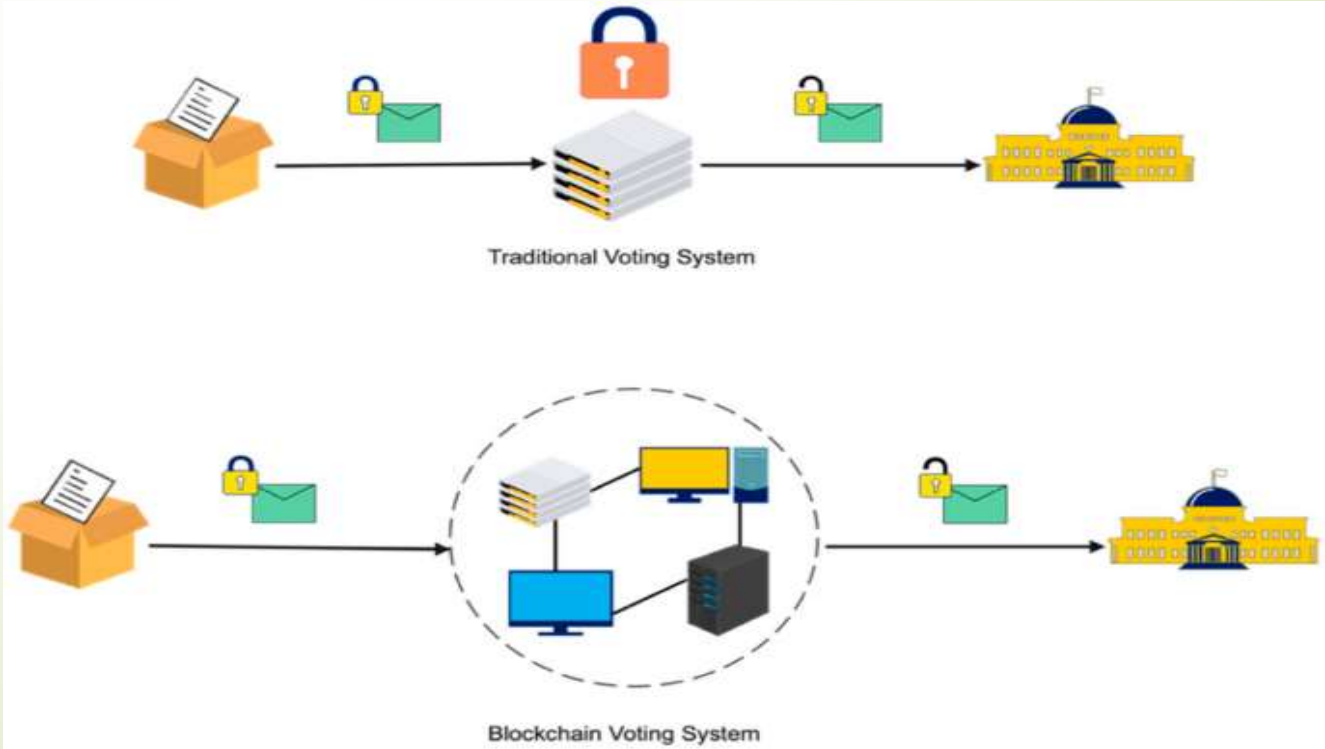
Guide: Mr. P. Purushotham

Introduction to Blockchain

- Blockchain is a decentralized, distributed ledger technology.
- Ensures data integrity, transparency, and security.
- Each block contains a cryptographic hash of the previous block.
- Applications: finance, supply chain, healthcare, and voting.

Problem Statement

• Traditional voting systems have fraud risks, security flaws, and lack transparency.
• Digital systems lack immutability and are prone to cyberattacks.
• Manual processes are error-prone and centralized control raises concerns.
• Blockchain voting enhances security, transparency, and accessibility.



Abstract

• A blockchain-based voting system using Java, JSP, and MySQL.
• Immutable, tamper-proof vote recording with blockchain.
• Voter authentication via biometric/OTP prevents duplicate votes.
• Smart contracts automate vote tallying and eligibility verification.
• Decentralized structure eliminates single points of failure.
• QR code-based ballots enhance security and usability.

Objectives

1. Develop a decentralized, tamper-proof voting system.
2. Implement voter authentication and anonymity mechanisms.
3. Ensure real-time result transparency and auditability.
4. Enhance security against cyber threats and fraud.
5. Provide a user-friendly interface for voters and administrators.

Applications of Blockchain in Voting

- Secure and transparent electoral processes.
- Prevents voter fraud and duplicate voting.
- Enables remote voting while maintaining security.
- Reduces reliance on centralized authorities.
- Provides immutable audit trails for election verification.

SWOT Analysis

Strengths:
- High security, transparency, and trust.
- Decentralized and immutable data.

Weaknesses:
- Scalability concerns.
- Requires internet and technical literacy.

Opportunities:
- Can be expanded for corporate or institutional voting.
- Potential integration with national election systems.

Threats:
- Resistance from traditional electoral authorities.
- Possible regulatory challenges.

System Architecture

- Frontend: JSP-based user interface.
- Backend: Java-based business logic.
- Blockchain: Secure ledger for vote storage.
- Database: MySQL for voter credentials.
- Security: Encryption, smart contracts, biometric/OTP verification.

Challenges and Future Scope

Challenges:

- Adoption barriers and regulatory hurdles.
- Scalability for national elections.
- Internet dependency in rural areas.

Future Scope:

- Integration with government electoral systems.
- AI-driven fraud detection.
- Expanding to corporate elections.

Conclusion

- Blockchain-based voting enhances security and transparency.
- Eliminates vulnerabilities like voter fraud and centralized control.
- Smart contracts ensure fair vote tallying.
- Future developments can make online voting mainstream and more accessible.