Memory & Computation-aware Trustworthy University e-Voting Solution - Solidity Approach

[1]Mr. K Purushotham , [2]C Snehitha , [3]B Raja sekhar , [4]B Harsha Vardhan sivateja, [5]A Sandeep Reddy , [6]D Lokesh

[1] Assistant Professor, M.tech., Department of Electronics and Communication Engineering, Sri Venkatesa Perumal college of Engineering and Technology, Andhra Pradesh, India

[2,3,4,5,6] UG scholar, Department of Electronics and Communication Engineering, Sri Venkatesa Perumal college of Engineering and Technology, Andhra Pradesh, India

ABSTRACT

The COVID-19 pandemic highlighted the need for safe and remote solutions, especially in processes that traditionally require physical presence, like voting. This paper presents a blockchain-based remote voting system designed specifically for university elections. The system aims to ensure security, anonymity, irreversibility, accessibility, and ease of use, allowing students to cast their votes without being physically present.

Unlike traditional electronic voting systems that rely on centralized control and are vulnerable to manipulation and double voting, the proposed system uses a ***permissioned blockchain*** *to enhance efficiency, reduce power consumption, and lower latency. By incorporating* ***smart contracts****, the platform ensures that all votes are securely recorded, publicly verifiable, and tamper-proof, while maintaining voter privacy.*

This solution leverages enterprise blockchain technology to provide a trustworthy and transparent voting process. It also offers a flexible network configuration that addresses key security and reliability challenges faced by conventional e-voting systems. Overall, the system offers a robust, scalable, and reliable alternative for conducting secure university elections.

Keywords: *Blockchain, electronic voting, university elections, smart contracts, permissioned blockchain, remote voting, anonymity, security, transparency, decentralized systems.*

1.INTRODUCTION:

1.1. GENERAL SYSTEM:

In recent years, the evolution of digital technologies has revolutionized traditional processes, enabling automation, transparency, and improved efficiency across various sectors. Voting systems, a fundamental pillar of democracy and institutional governance, have also experienced this digital shift. However, the emergence of the COVID-19 pandemic exposed critical gaps in conventional voting mechanisms, emphasizing the urgent need for remote, secure, and verifiable alternatives that ensure voter safety without compromising integrity.

Electronic voting (e-voting) systems have been introduced to address these concerns, but most existing solutions are built on centralized infrastructures. These centralized models are prone to several vulnerabilities, including single points of failure, unauthorized data manipulation, and reduced transparency. In particular, university-level elections require a solution that balances security, accessibility, ease of use, and integrity, especially in environments where voters are distributed and remote participation is essential.

This paper introduces a blockchain-based e-voting system, specifically designed for university elections, that leverages **permissioned blockchain architecture** and **smart contracts** developed in Solidity. Unlike public blockchains that require extensive computational resources and introduce latency, the use of permissioned blockchain in this system enhances performance while maintaining cryptographic security and auditability.

The proposed system ensures **voter anonymity**, prevents **double voting**, provides **irreversibility**, and facilitates **real-time result transparency**. It addresses fundamental issues in traditional voting by storing each vote as a secure transaction on the blockchain, protected by asymmetric encryption and validated through an efficient consensus mechanism. Additionally, it allows flexible network configuration and ensures that only eligible voters can access and cast their votes using verified credentials.

By integrating blockchain technology into academic election environments, this approach aims to deliver a trustworthy, scalable, and tamper-resistant voting platform that upholds the democratic principles of fairness, accuracy, and privacy.

1.2 :APPROACHES OF E-VOTING

1. Traditional Approaches to E-Voting (Non-Blockchain)

- **Centralized Voting Systems**: These are the conventional online voting systems where a central authority handles vote collection, tallying, and results. However, they suffer from issues like:
    - Vulnerability to hacking
    - Lack of transparency
    - Risk of vote manipulation

2. Blockchain-Based E-Voting

This is the core focus of your document. Blockchain introduces decentralization, transparency, and security to e-voting.

The key approaches within this model include:

a. Proof of Work (PoW)

- A consensus mechanism where computational power is used to validate transactions (votes).
- It ensures data integrity but is resource-intensive and slow, making it less ideal for large-scale voting in real-time.

b. Proof of Authority (PoA)

- A more efficient consensus model where only approved nodes (authorities) can validate votes.
- It's faster and more energy-efficient than PoW, though slightly more centralized.

3. Hybrid Approaches

- Combining blockchain with biometric authentication or national ID systems.
- Utilizing smart contracts (e.g., on Ethereum) to automate voting procedures and ensure trust.

1.3 DOMAIN OVERVIEW

The domain of this project falls under e-Governance and electronic voting systems, where the goal is to ensure secure, transparent, and tamper-proof elections using modern technology. With the traditional voting mechanisms facing challenges such as electoral fraud, lack of transparency, and high costs, the adoption of electronic and blockchain-based voting is gaining attention.

Electronic voting (e-voting) provides the ability to cast votes via electronic means, either through kiosks or remotely over the internet. While e-voting can streamline the voting process and increase accessibility, it introduces concerns related to data security, authentication, voter privacy, and trust.

To address these challenges, blockchain technology is introduced as a foundational element. Blockchain is a decentralized, immutable ledger that can store voting records securely. Each vote is treated as a transaction and recorded on a public ledger that can be audited but not altered. This ensures:

- **Transparency** – all parties can view and verify vote counts.
- **Security** – the use of cryptographic techniques ensures tamper-resistance.
- **Anonymity** – voters can cast their vote without revealing their identity.
- **Decentralization** – removes single points of failure or manipulation.

The integration of blockchain into e-voting also allows the use of **smart contracts**, which are self-executing programs that automate processes like vote validation, result tallying, and fraud detection.

2: METHODOLOGY

This research presents a decentralized and secure framework for university-level electronic voting using blockchain technology and smart contracts. The methodology is organized into distinct stages: system design, cryptographic security, blockchain integration, smart contract implementation, vote casting and validation, and result publication. Each phase ensures transparency, integrity, and user privacy in the voting process.

1. System Design and Architecture

The system architecture is designed to separate concerns, assign distinct roles, and prevent tampering:

- **Client Interface**: Allows voters to interact with the voting system.
- **Application Layer**: Handles authentication, encryption, and validation of votes.
- **Blockchain Layer**: Records votes as transactions in an immutable ledger.
- **Database Layer**: Stores public results but not voter identity or raw votes.

The design utilizes **UML diagrams** to model interactions between entities like voters, the voting committee, and the blockchain system, formalizing the conceptual architecture.

2. Cryptographic Security and Authentication

To ensure voter anonymity and system integrity, multiple cryptographic techniques are employed:

- **Token-Based Authentication**: Each voter is issued a unique token and PIN.
- **Encrypted Vote Identifier**: Generated at the application level to prevent traceability.
- **Public-Private Key Infrastructure (PKI)**: Secures communication and data exchange between nodes.

These measures ensure the authenticity of users and the confidentiality of their votes.

C. Blockchain Integration

A **consortium blockchain model** is used for better control, speed, and energy efficiency:

- **Permissioned Blockchain**: Only validated university nodes can add transactions.
- **Immutability**: Each vote recorded as a block cannot be altered or deleted.
- **Transparency**: All voting transactions are publicly viewable while maintaining voter anonymity.

This blockchain framework prevents unauthorized changes and ensures auditability.

D. Smart Contract Implementation

Smart contracts serve as the core logic of the voting system:

- **Candidate Listing and Vote Casting**: Encoded into the smart contract.
- **One-Person-One-Vote Logic**: Enforced via automated validation.
- **Result Tallying**: Performed automatically and published instantly post-election.

The contracts are developed using **Solidity** and deployed on the **Ethereum** platform, ensuring tamper-proof execution of election rules.

E. Voting and Validation Workflow

The voting process follows a secure, step-by-step protocol:

- Voter logs into the system using a valid token.
- The system checks if the user has already voted.

- Voter selects a candidate.
- Confirmation and validation are performed.
- The vote is recorded on the blockchain as a transaction.

This two-phase approach **voting and validation** adds an extra layer of protection against fraudulent entries.

F. Result Compilation and Display

Once voting ends, the smart contract automatically compiles the results:

- Results are recorded on the blockchain.
- Displayed in real-time to university authorities and voters.
- Eliminates the need for manual counting and reduces risks of manipulation.

G. System Performance and Integrity

The system is evaluated based on:

- **Security**: Ensures only valid voters can vote, and no vote duplication occurs.
- **Anonymity**: No link is maintained between voters and their choices.
- **Transparency**: Voting transactions are verifiable by any node in the network.

The architecture supports scalability, adaptability, and compliance with institutional election standards.

3.EXPERIMENTAL DETAILS

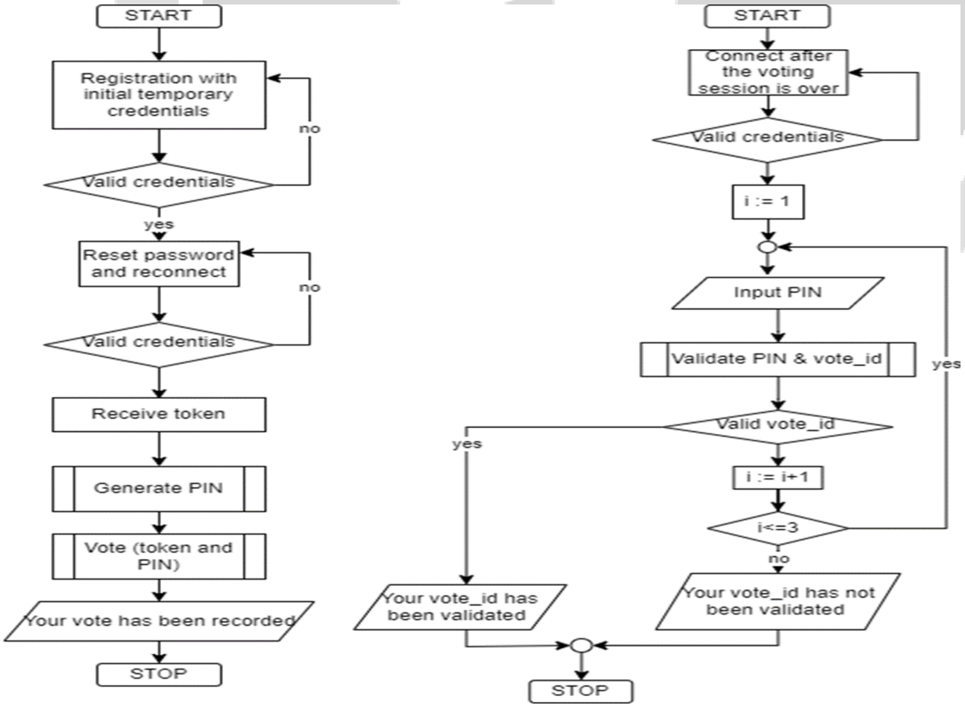
START
Registration with initial temporary credentials
Valid credentials
no
yes
Reset password and reconnect
Valid credentials
no
Receive token
Generate PIN
Vote (token and PIN)
Your vote has been recorded
STOP
START
Connect after the voting session is over
Valid credentials
i := 1
Input PIN
Validate PIN & vote_id
yes
Valid vote_id
yes
i := i+1
i<=3
no
Your vote_id has been validated
Your vote_id has not been validated
STOP

Fig 1: Proposed system architecture

- **Left Side:** Voter Registration and Voting Process

- **Start:** The process begins when a voter tries to register or log in.
- **Use Temporary Credentials:** The voter uses some initial, temporary login information.
- **Are Credentials Valid?:** The system checks if these initial credentials are correct.
- **No:** If the credentials are wrong, the voter is sent back to the beginning and needs to register/log in again.
- **Yes**: If the credentials are correct, the process continues**.**
- **Reset Password and Reconnect**: For security, the voter is asked to create a new, permanent password. They then need to log in again with this new password**.**
- **Are Credentials Valid?:** The system checks the new password.
- **No**: If the new password is wrong, the voter has to reset it and try logging in again.
- **Yes:** If the password is correct, the process continues**.**
- **Receive Token:** The system gives the voter a unique "token." This is like a special key that proves they are logged in and authorized to vote**.**
- **Generate PIN:** The system creates a Personal Identification Number (PIN) specifically for this voting session. This adds another layer of security**.**
- **Cast Vote:** The voter submits their vote, along with the token and the PIN. This is how the system knows it's really them casting the vote.
- **Record Vote:** The system securely records the voter's choice.
- **End:** The voting process is complete for this voter.
- **Right Side**: Vote Validation Process
- This part happens after the voting is finished. It's about making sure the votes that were cast are valid.
- **Connect to Voting Data:** The system connects to the database or blockchain where the votes are stored.
- **Are Credentials Valid?:** The system checks the credentials used to access the voting data. This is likely done by authorized personne**l.**
- **i = 1:** A counter variable 'i' is set to 1.
- This is likely used to limit the number of attempts to validate a vote.
- **Input PIN**: The system takes a PIN as input. This PIN would be associated with a specific vote.
- **Validate PIN and vote_id:** The system checks if the PIN and the vote_id (a unique identifier for each vote) match. This is a crucial step to ensure the vote is legitimate**.**
- **Yes (vote_id Validated):** The system confirms that the vote is valid**.**
- **No (vote_id Invalid):** The system increases the counter 'i'.
- **i <= 3?:** The system checks if the counter 'i' is less than or equal to 3. This means there are a limited number of attempts to validate a vote.
- **Yes:** If 'i' is still within the limit, the process goes back to step 5 (Input PIN) to try again.
- **No (vote_id Not Validated):** If the maximum number of attempts is reached and the vote is still invalid, the vote is marked as "not validated." This might indicate a problem wit the vote, and it would need further investigation.
- **End:** The vote validation process is complete**.**

4.CONCLUSION

The digital voting system described ensures a highly secure and structured approach to conducting elections. It is divided into two main phases: the voter registration and voting process, and the vote validation process. In the first phase, voters begin by logging in with temporary credentials, which are then verified by the system. To strengthen security, voters are required to reset their password and log in again using the new credentials. Once authenticated, they receive a unique token and a system-generated PIN. These serve as additional layers of verification and are used when the voter casts their ballot. The vote is then securely recorded in the system, ensuring that only authorized individuals are able to participate in the election.

The second phase focuses on validating the authenticity of each vote. Authorized personnel access the voting database and use the stored PIN and vote ID to verify each vote. The system allows up to three attempts to validate a vote. If the credentials do not match within these attempts, the vote is marked as “not validated,” signaling a potential issue that may require further investigation. This process helps maintain the integrity of the election by ensuring that only valid and legitimate votes are counted.

Overall, the system provides a strong and reliable digital voting framework by combining multiple layers of user authentication with strict post-voting validation. This approach safeguards against unauthorized access, vote tampering, and fraud. By ensuring that both the act of voting and the process of validating votes are secure, transparent, and auditable, the system builds trust among voters and upholds the principles of democratic integrity in an electronic environment.

5.REFERENCES

- Simona-Vasilica Oprea, Adela BÃ¢ra ,Anca-Ioana Andreescu, Marian Pompiliu Cristescu Conceptual Architecture of a

  Blockchain Solution for E-Voting in Elections at the University Level IEEE Access, 2023
- Geetanjali Rathee, Razi Iqbal, Omer Waqar, Ali Kashif Bashir On the Design and Implementation of a Blockchain Enabled

  E Voting Application Within IoT-Oriented Smart Cities IEEE Access, 2021
- Shiyao Gao, Dong Zheng, Rui Guo, Chunming Jing, Chencheng Hu An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function IEEE Access, 2019
- Ali Benabdallah, Antoine Audras, Louis Coudert, Nour El Madhoun, Mohamad Badra Analysis of Blockchain Solutions for E Voting: A Systematic Literature Review IEEE Access, 2022
- Myungsun Kim Toward Round-Efficient Verifiable Re-Encryption Mix-Net IEEE Access, 2022
- Huy Quoc Le,Bay Vo,Dung Hoang Duong,Willy Susilo,Ngoc T. Le,Kazuhide Fukushima,Shinsaku Kiyomoto IdentityBased Linkable Ring Signatures From Lattices IEEE Access, 2021
- Kanika Agrawal,Mayank Aggarwal,Sudeep Tanwar,Gulshan Sharma,Pitshou N. Bokoro,Ravi Sharma An Extensive

  Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions IEEE Access, 2022
- Basit Shahzad,Jon Crowcroft Trustworthy Electronic Voting Using Adjusted Blockchain Technology IEEE Access, 2019
- Muhammad Shoaib Farooq,Usman Iftikhar,Adel Khelifi A Framework to Make Voting System Transparent Using Blockchain Technology IEEE Access, 2022
- Wang Rong-Bing,Li Ya-Nan,Xu Hong-Yan,Feng Yong,Zhang Yong-Gang Electronic Scoring Scheme Based on Real Paillier Encryption Algorithms IEEE Access, 2019
- Quang Nhat Tran,Benjamin P. Turnbull,Hao-Tian Wu,A. J. S. de Silva,Katerina Kormusheva,Jiankun Hu A Survey on PrivacyPreserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture IEEE Open
  Journal of the Computer Society, 2021
- A. Y. Chang, K. Cowling, A. E. Micah, A. Chapin, C. S. Chen, G. Ikilezi, et al., Past present and future of global health financing: A review of development assistance government out-of-pocket and other private spending on health for 195 countries 1995â€“2050, Lancet, vol. 393, pp. 2233-2260, Jun. 2019.
- A. I. Sanka and R. C. C. Cheung, A systematic review of blockchain scalability: Issues solutions analysis and future research, J. Netw. Comput. Appl., vol. 195, Dec. 2021.
- M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah and R. Jayaraman, Scalable blockchainsâ€"A systematic review, Future Gener. Comput. Syst., vol. 126, pp. 136-162, Jan. 2022.
- N. Mohd. Suki and N. Mohd. Suki, Decision-making and satisfaction in campus e-voting: Moderating effect of trust in the system, J. Enterprise Inf. Manage., vol. 30, no. 6, pp. 944-963, Oct. 2017.
- S. Squarepants, Bitcoin: A peer-to-peer electronic cash system, SSRN Electron. J., pp. 21260, Jun. 2008.

- T. Aste, P. Tasca and T. D. Matteo, Blockchain technologies: The foreseeable impact on society and industry, Computer, vol. 50, no. 9, pp. 18-28, Jan. 2017.
- M. Volkamer, O. Spycher and E. Dubuis, Measures to establish trust in Internet voting, Proc. 5th Int. Conf. Theory Pract. Electron. Governance, pp. 1-6, 2011.