SMART CONTRACT BASED SECURE VOTING SYSTEM

Komal Mehta	Prasant Kumar	Arpit Raj
Apex Institute Of Technology	BE CSE -BCT	BE CSE -BCT
Chandigarh University	Chandigarh University	Chandigarh University
Mohali, India	Mohali,India	Mohali,India
komal.e15888@cumail.in	22BCT10071@CUCHD.IN	22BCT10064@CUCHD.IN

Abstract— Blockchain has already been used in developing many applications, including cryptocurrencies and NFTs. With the help of blockchain and smart contracts, a Decentralized E-Voting System can be developed. A Decentralized E-Voting System is used for activities like voting, verifying the user's details, adding candidates, starting and ending the election, self-tallying the total number of votes, and giving the results of the elections. A system using blockchain is more secure, faster, transparent, and immutable. The existing systems for voting are less secure as they use EVMs and VVPATs, which can be tampered with. The existing systems are also slower than the proposed model in terms of the time taken to announce the results. There are other problems like Vote Rigging, Polling Booth Capture, and Voting Manipulation. With the increasing risk of cyberattacks, it is of utmost importance to have an online voting system capable of withstanding these attacks. A blockchain-based e-voting system will enable user confidentiality using encryption. The platform is created on the Ethereum network that makes use of smart contracts written in the Solidity programming language. Truffle, Ganache and Metamask are the tools used to create a Decentralized E-Voting System.

Introduction

In the dynamic landscape of technological advancement, electronic voting systems have emerged as a promising solution to modernize and streamline the electoral process. These systems offer voters the convenience of casting their ballots from anywhere, using a variety of electronic devices such as smartphones or computers. However, despite significant research and development in this field, widespread adoption of electronic voting systems has been hindered by concerns surrounding their security and integrity.

Traditional electronic voting systems have faced criticism due to vulnerabilities that could compromise the secrecy and accuracy of votes. Issues such as hacking, tampering, and manipulation have raised doubts about the reliability of these systems. Consequently, governments and electoral authorities have been cautious about implementing electronic voting on a larger scale, fearing the potential consequences of security breaches.

In this paper, we explore the potential of blockchain technology to address these challenges and revolutionize the electronic voting landscape. Blockchain, renowned as the underlying technology behind cryptocurrencies like Bitcoin, provides a decentralized and secure platform for digital transactions. Its core principles of transparency, immutability, and cryptographic security make it an ideal solution for safeguarding the integrity of electronic voting systems.

By harnessing blockchain technology, we aim to design an electronic voting system that ensures the anonymity of voters, maintains transparency throughout the voting process, and provides robust protection against tampering and fraud. This paper delves into the fundamentals of blockchain technology, its application in electronic voting, and the potential benefits it brings to the electoral process.

Through our research and analysis, we seek to demonstrate how blockchain-based electronic voting systems can overcome the security concerns that have hindered the widespread adoption of electronic voting. By leveraging the power of blockchain, we envision a future where voting becomes more accessible, transparent, and trustworthy, thereby strengthening democracy and fostering civic engagement.

II. Literature Review

A.Votereum: An Ethereum-based E-voting system:
- Creators: Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen
- Institution: College of Data Innovation Vietnam National College HCMC, Vietnam

- Description: Proposes Votereum, an e-voting system leveraging blockchain technology, particularly powered by the Ethereum platform. The system includes one server managing the entire system and another handling blockchain-related requests.

B.Online Voting: Voting Framework Utilizing Blockchain:

- Creators: Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure, Pranali Shirke Prasad Halgaonkar
- Description: Provides a brief survey of different methodologies used in current voting systems. Aims to build a system capable of addressing present and upcoming challenges and eliminating drawbacks from past architectures.

C.Decentralized Voting Stage Based on Ethereum Blockchain:

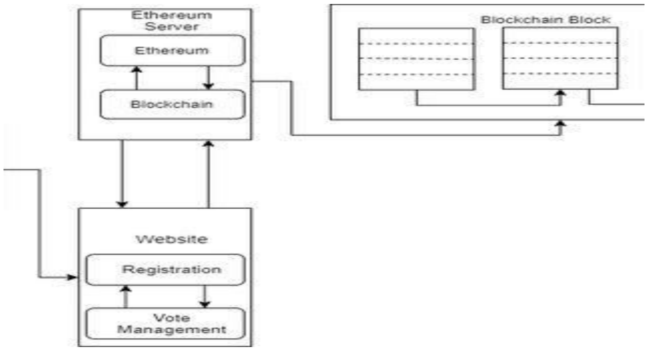
- Creators: David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb
- Institution: Office of Computer Science, American College of Science and Technology
- Description: Proposes a decentralized trustless voting platform based on blockchain technology, specifically utilizing the Ethereum Virtual Machine (EVM) for data integrity, transparency, and security in voting.

D.Overview on Blockchain Based E-Voting Recording Framework Design:

- Creator: G. Bhavani
- Description: Discusses the adoption of blockchain in e-voting systems to reduce database manipulation and improve security. Utilizes the AES algorithm for encrypting data from fingerprint sensors and discusses recording voting results using blockchain algorithms.

E. Blockchain-Based E-Voting System:

- Creators: Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson
- Institution: School of Computer Science, Reykjavik College, Iceland
- Description: Evaluates the potential of distributed ledger technologies through a case study on election processes. Implements a blockchain-based application to enhance security and reduce the cost of hosting nationwide elections.



PROPOSED SYSTEM

The simple rationalization could be a 'chain' of blocks. A block is associate degree mass set of information. knowledge square measure collected and methoded to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

WORKING :

The SHA-256 algorithm is a crucial component of blockchain technology, as it plays a fundamental role in ensuring the integrity and security of data stored within blocks. This algorithm possesses several key properties that make it well-suited for cryptographic applications:

1. Deterministic: Regardless of how many times the same input is entered, the SHA-256 algorithm will consistently produce the same output. This deterministic nature is essential for maintaining the reliability and predictability of cryptographic operations.

2.Quick Computation: The SHA-256 algorithm is designed to generate output rapidly, contributing to the overall efficiency of the system. This quick computation allows for timely processing of data, enhancing the performance of blockchain networks.

3. Pre-Image Resistance: Pre-image resistance refers to the difficulty of determining the original input from its hash value. In the context of blockchain, this property ensures that even if the hash value of a block is known, it is computationally infeasible to reverse-engineer the

original data. This resistance to pre-image attacks strengthens the security of blockchain systems.

4. Small Changes in Input Change the Whole Output: A minor alteration to the input data results in a significantly different output hash value. This property, known as the avalanche effect, ensures that even subtle modifications to the data will produce drastic changes in the resulting hash, making it virtually impossible to predict or manipulate.

5. Collision Resistance: Every input is mapped to a unique hash value, reducing the likelihood of two different inputs producing the same hash. Collision resistance is critical for maintaining the integrity and authenticity of data stored in blockchain transactions.

6. Puzzle Friendly: The SHA-256 algorithm exhibits puzzle-friendliness, meaning that combining two values results in a unique hash value for the composite variable. This property enables the creation of complex cryptographic puzzles and challenges within blockchain networks.

In the context of blockchain technology, hashing serves as a foundational mechanism for ensuring the immutability and security of the distributed ledger. Each block in the blockchain contains a hash pointer that references the hash value of the previous block, forming a continuous chain of blocks. This interconnected structure makes it exceedingly difficult for malicious actors to tamper with individual blocks without affecting the entire chain. As a result, the blockchain concept revolutionizes data integrity and trust in digital transactions, paving the way for innovative applications across various industries.

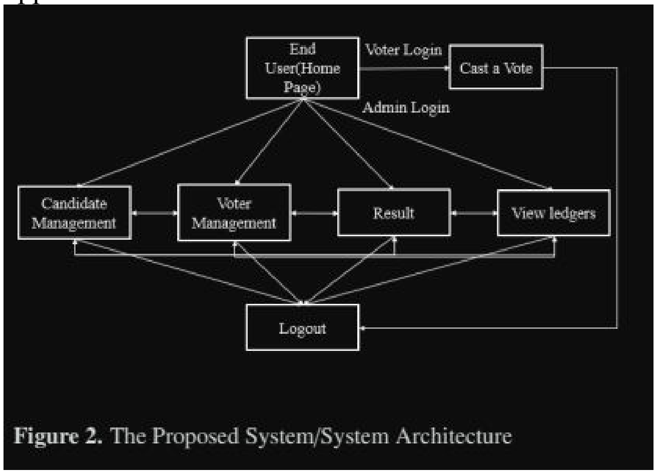


Figure 2. The Proposed System/System Architecture

METHODOLOGY

Ensuring the integrity of the voting process begins with robust voter registration procedures. In our plan, we prioritize identity verification to prevent fraudulent activities, especially crucial in elections where each vote carries significant weight. Our proposed system utilizes Recognition devices and valid ID numbers to verify voter eligibility and presence in the database. Upon successful verification, each voter receives a unique hash address, along with Ethers to cast a single vote securely.

On election day, voters undergo a verification process at polling booths. Using their assigned hash addresses, they proceed to cast their votes securely. Once the vote is cast, voters are automatically logged out of the system. Additionally, they receive live updates on the voting progress.

This section delves into the technical details of our proposed system, which comprises two main subsystems: the registration system and the voting system.

Our registration system employs a front-end interface in HTML/CSS and a back-end database in SQL. It securely stores users' personal details, akin to an Aadhar database. Biometric devices are utilized for validation, and upon successful verification, users are provided with hash codes/addresses as their login credentials for accessing the voting machine.

The voting system functions as a decentralized application (DApp), with a front-end interface built using Bootstrap or HTML and a blockchain backend. Smart contracts, written in Solidity, govern the voting process securely. Each change in the blockchain, known as a transaction, incurs a transaction fee paid in Ether, the native currency of the Ethereum network. Ganache-CLI facilitates the setup of a private network for accelerated development and testing, while MetaMask serves as a browser-based interface for interaction with Ethereum dApps.

Our proposed e-voting framework harnesses innovative technologies such as blockchain and biometrics to ensure the security, transparency, and efficiency of electoral processes. By adhering to rigorous registration and voting protocols, we aim to foster trust and participation in democratic governance.

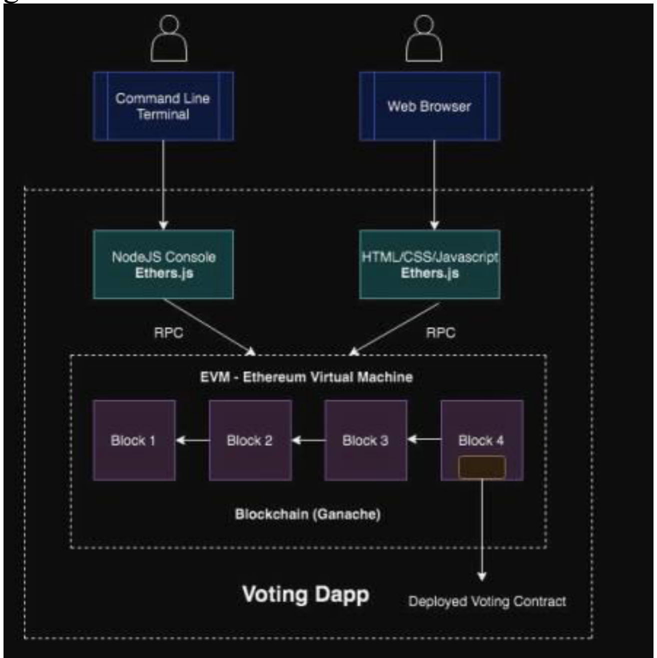


Fig. 1 Proposed system architecture

VI. Results And Conclusion

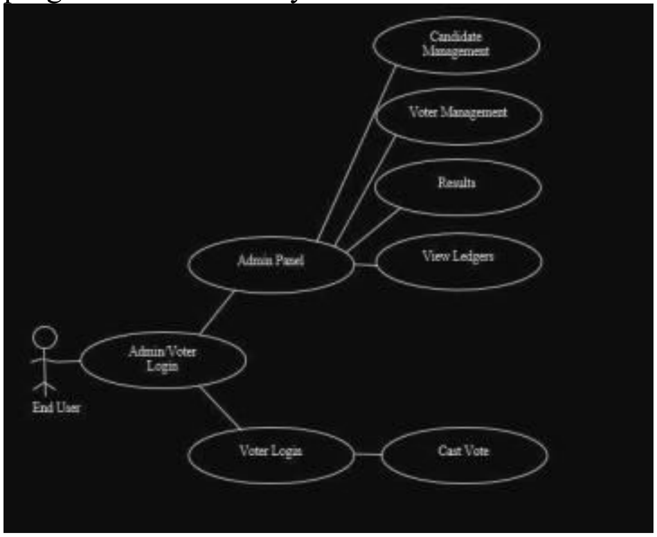
In our pioneering endeavor, we've unveiled a visionary electronic voting framework rooted in blockchain technology. By harnessing the power of smart contracts, we've crafted a solution that not only ensures the sanctity of elections but also safeguards the privacy of voters, all while remaining remarkably cost-effective.

Through meticulous research and development, we've demonstrated that blockchain offers a promising avenue for overcoming the longstanding limitations and adoption challenges of electronic voting systems. Our framework, built on an Ethereum private blockchain, boasts the capacity to handle hundreds of transactions per minute, leveraging smart contracts to alleviate the strain on the blockchain infrastructure.

For nations with larger populations, we've identified the need for additional measures to support increased transaction throughput. Nevertheless, the inherent transparency of blockchain technology paves the way for enhanced auditing and understanding of electoral processes, aligning seamlessly with the fundamental requirements of a robust voting system.

These attributes, stemming from the decentralized nature of blockchain networks, have the potential to further democratize elections, particularly in direct democracy systems. To usher in a new era of openness, transparency, and accountability in e-voting, blockchain emerges as a compelling solution.

Our project serves as an exploration of the boundless potential of blockchain technology in the realm of electronic voting. With a publicly verifiable and incorruptible distributed ledger, we ensure that the integrity of the voting process remains uncompromised. It's not just a technological advancement; it's a beacon of progress for democracy itself.



.

VII. Future Scope

Embarking on a journey toward improved efficacy and potency of our e-voting system involves several key advancements:

Firstly, reinforcing our verification process with the Aadhar number confirmation system ensures that only qualified voters engage in the electoral process.

Moreover, establishing a seamless connection between our application and Government voting data offers access to a comprehensive voter repository, validating the integrity of our democratic proceedings.

To fortify our system's robustness, enhancing our security measures is imperative. This ensures resilience against potential threats, fostering unwavering confidence in the reliability and integrity of our platform.

Revamping our Graphical User Interface (GUI) enriches user interaction and accessibility, facilitating a more intuitive and user-friendly voting experience.

Incorporating local dialects into our application promotes engagement among rural and less educated populations, fostering inclusivity and broadening accessibility.

Empowering voters with comprehensive insights into candidates' backgrounds and qualifications cultivates an informed electorate, facilitating sound decision-making.

Introducing a feedback mechanism enables public participation, offering valuable insights and recommendations to elected representatives, thus nurturing a culture of accountability and responsiveness.

Lastly, implementing a robust complaint system empowers individuals to flag any irregularities or infringements during the electoral process, reinforcing transparency and fairness in our democratic practices.

REFERENCES

1. Emre Yavuz, Ali Kaan Koç, Umut Can Çabuk, and Gökhan Dalkılıç (2018) blazed a trail "Towards secure e-voting utilizing Ethereum blockchain", ushering in advancements in security and integrity within electronic voting systems.

2. KC Tam (2018) delved into the intricacies of "Exchanges in Ethereum", shedding light on the complex processes within the Ethereum blockchain that underpin secure transactions.

3. The indispensable role of Metamask cannot be overstated in facilitating interaction with blockchain systems, serving as a vital conduit between users and decentralized applications.

4. David Khoury, Elie F. Kfoury, Ali Kassem, and Hamza Harb (2018) advocated for a "Decentralized Voting Stage Based on Ethereum Blockchain", presenting a novel approach to trustless voting systems.

5. Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure, and Pranali Shirke Prasad Halgaonkar (2019) introduced an "Online Voting: Voting Framework Utilizing Blockchain", offering an innovative solution to address challenges in traditional voting architectures.

6. Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, and Tuan A. Nguyen (2019) advanced with "Votereum: An Ethereum-based E-voting framework", leveraging blockchain innovation to enhance the efficiency and security of electronic voting processes.

7. G Bhavan (2018) conducted a comprehensive "Overview on Blockchain Based E-Voting Recording Framework Plan", providing valuable insights into the landscape of blockchain-based e-voting solutions.

8. Friðrik Þ. Hjálmarsson and Gunnlaugur K. Hreiðarsson (2018) significantly contributed to the field with their work on a "Blockchain-Based E-Voting Framework", promoting a secure and transparent platform for conducting elections.

9. Rifa Hanifatunnisa and Budi Rahardjo (2017) presented their work on a "Blockchain Based E-Voting Recording Framework", contributing to the advancement of secure and auditable e-voting solutions.

10. Supriya Thakur Aras and Vrushali Kulkarni (2017) conducted a detailed survey on "Blockchain and Its Applications", offering insights into the diverse applications of blockchain technology, including its potential in e-voting systems.

11. Saravanan Raju, Sai Boddepalli, Suraj Gampa, Qiben Yan, and Jitender S. Deogun (2017) explored "Character administration utilizing blockchain for cognitive cellular systems", showcasing the versatility of blockchain beyond e-voting systems.

13. Venkata Naga Rani B, Akshay S, Arun Kumar M, and Ishwar Kumar M A (2019) presented their work on a "Decentralized E-Voting Framework", adding to the growing body of research on secure and transparent electronic voting solutions.