Blockchain Voting with Tamper Verification using Telegram Bot

M.Harshath¹, S.LingaPrabu², E.Prabhakar³, R.Mohanraj⁴, R.Vignesh⁵
¹,²,⁴,⁵ UG-Computer Science and Engineering, Nandha College of Technology, Erode, TamilNadu
³ Assistant Professor - Computer Science and Engineering, Nandha College of Technology, Erode, TamilNadu

Orcid ID: https://orcid.org/0009-0001-2802-3656

ABSTRACT
Blockchain technology has the potential to revolutionize the voting process by providing a secure and transparent method for recording votes. This paper proposes a voting system that utilizes blockchain technology, along with the Django web framework and Django administration for user profile updates, login using Aadhar number. The system incorporates a unique login feature that utilizes an Aadhar number, and two-step authentication through email OTP and private key authentication. The use of Merkle trees and SHA ensures a proof of work that prevents double voting, while tamper verification is achieved through a Telegram bot. The proposed system provides a secure, transparent, and efficient method for conducting elections, which is essential for ensuring a fair and democratic society.


I. Introduction:
Voting is a fundamental right in democratic societies, and ensuring the integrity and security of voting systems is of utmost importance. Traditional paper-based voting systems are increasingly being replaced by electronic voting systems that leverage the power of technology to make voting more efficient and accessible. However, electronic voting systems are prone to security risks and tampering, which can undermine the validity and integrity of the voting process. Blockchain technology offers a potential solution to these problems by providing a secure and transparent platform for electronic voting.

The proposed voting system aims to leverage blockchain technology to enhance the transparency and security of the electoral process. The system's frontend will be developed using Django, a popular web framework for building scalable and secure web applications. Users will be required to log in using their Aadhar number, which is a unique identification number issued to every Indian resident. The Aadhar number serves as the primary identification mechanism for the users, ensuring that only eligible voters can cast their votes.

To prevent unauthorized access and ensure secure voting, the system will incorporate two-factor authentication (2FA) using mail OTP and private key authentication. The mail OTP will be sent to the user's registered email address. After successful authentication using mail OTP and before proceeding with vote, users will be prompted to enter their private key, which is a cryptographic code that is unique to every user. The private key serves as an additional layer of security, making it difficult for hackers to tamper with the voting process.

To ensure the authenticity and security of the votes, a telegram bot will be integrated into the system. The telegram bot will verify that each vote is genuine and has not been tampered with. The telegram bot will work by generating a hash value of the vote, which is a unique code that represents the vote's contents. The hash value will be compared to the hash value stored on the blockchain, ensuring that the vote has not been altered or manipulated.

Overall, the proposed voting system will provide a secure and transparent mechanism for casting votes. By leveraging blockchain technology, the system ensures that the voting process is tamper-proof, and the results are immutable. The use of two-factor authentication and private key authentication provides an additional layer of security, preventing unauthorized access and ensuring
secure voting. The integration of the telegram bot provides an additional mechanism for verifying the authenticity of the votes, making the system more reliable and trustworthy.

II. Related Work:
The proposed online voting system in the paper [1] incorporates a client-server model with a user-friendly interface that can handle large volumes of data. The paper emphasizes the importance of maintaining the confidentiality and integrity of the voting process, which is ensured by using encryption techniques and digital signatures to protect the data. The paper also explains how the system provides real-time results that can be viewed by authorized individuals, which can speed up the electoral process and enhance transparency. Overall, the proposed online voting system aims to improve the accuracy, security, and convenience of the voting process, making it a promising solution for modern elections.

The Authors [2] of the paper proposing a Cloud technology that offers a secure and reliable platform for conducting elections. The system uses a three-tier architecture with a user interface, processing layer, and database layer to store all election-related data. The system incorporates multiple security measures, including encryption, multi-factor authentication, and intrusion detection, to prevent any unauthorized access or tampering. The proposed system offers increased accessibility, reduced costs, improved accuracy, and scalability, making it suitable for elections of any scale. Overall, the system has the potential to revolutionize the way elections are conducted by overcoming the challenges posed by traditional paper-based voting systems.

The proof-of-concept paper [3] presented by Fáber D. Giraldo, Barbosa Milton C., and Carlos E. Gamboa proposes an electronic voting system using Blockchain technology and Smart Contracts. The system uses a permissioned Blockchain network to store all the election-related data and incorporates various security measures to prevent unauthorized access or tampering. The proposed system offers benefits such as increased transparency, reduced costs, and improved accuracy and reliability. The system is scalable and can accommodate a large number of voters, making it suitable for elections of any scale. Overall, the proposed system has the potential to revolutionize the way elections are conducted by ensuring transparency, security, and integrity of the voting process.

The article [4] "A quick look at Cryptocurrency Mining: Proof of Work" by Rohit Beer and Tarunim Sharma provides an overview of the Proof of Work (PoW) consensus algorithm used in cryptocurrency mining. The authors explain the concept of PoW and how it is used to validate transactions on the blockchain network. They also describe the mining process, including the hardware and software used by miners to solve complex mathematical equations and add new blocks to the blockchain. The article also highlights the environmental concerns associated with PoW mining, particularly the high energy consumption required to power the mining hardware. Overall, the article provides a brief but informative introduction to the PoW consensus algorithm and its role in cryptocurrency mining.

The paper [5] "Toward a Green Blockchain: Engineering Merkle Tree and Proof of Work for Energy Optimization" proposes a new approach to optimize energy consumption in the blockchain network. The authors suggest using Merkle Tree and Proof of Work techniques to minimize the number of computations required for validating transactions, thus reducing energy consumption. They also present a novel method for verifying transactions using partial proofs, which further decreases computational requirements. The paper concludes that these techniques can significantly reduce energy consumption in the blockchain network without compromising security or performance.

"A Smart Contract System for Decentralized Borda Count Voting" paper [6] proposes a smart contract system that uses the Borda count method on the Ethereum blockchain platform for decentralized voting. The system ensures privacy and anonymity of users through cryptographic techniques and eliminates the need for intermediaries vulnerable to fraud. A simulation shows that the proposed system is more secure and efficient than traditional voting systems. The system has the potential to revolutionize the voting process by providing a secure, transparent, and efficient method of voting that can be used in a decentralized manner, overcoming the challenges of traditional voting systems.
The Authors of “A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT” [7] proposes a secure and transparent voting mechanism for decentralized IoT systems, utilizing blockchain technology and cryptographic techniques. The protocol creates a smart contract on the Ethereum blockchain to record votes and automatically validate the results through advanced cryptographic techniques, ensuring privacy, anonymity, and security of the voters. The simulations conducted show that the protocol is more efficient and secure than traditional voting systems, making it a viable alternative for future elections.

III. System Design:
III.1. Existing System
Centralized voting is a traditional approach to conducting elections where all the voting data is collected and processed by a central authority, such as a government agency or an independent election commission. While centralized voting has been used for decades and is well-established, it does have some drawbacks.

Ethereum-based blockchain voting refers to the use of the Ethereum blockchain platform to conduct secure and transparent voting. It allows users to cast their votes electronically using smart contracts that are programmed to execute specific voting rules. The process involves creating a digital identity for each voter and assigning them a unique identifier on the Ethereum blockchain. The voters can then cast their vote using their digital identity, which is encrypted to ensure anonymity.

Advantages & Disadvantages:
One of the main drawbacks of centralized voting is the potential for manipulation and fraud. Since all the voting data is controlled by a single authority, there is a risk of intentional or unintentional bias in the counting process, or of a single point of failure in the system, such as a hack or a malfunction. This can undermine the legitimacy of the election results and erode public trust in the electoral process.

Another disadvantage of centralized voting is the lack of transparency. Since the data is collected and processed by a single entity, there may be limited visibility into the process, making it difficult to verify the accuracy and integrity of the voting data. This can also contribute to mistrust in the election results.
The results of the vote are recorded on the blockchain, providing transparency and immutability to the process. Since the data on the blockchain is decentralized and tamper-proof, it eliminates the need for a central authority to oversee the voting process. However, there are challenges with blockchain-based voting, such as ensuring voter privacy and preventing hacking attempts. Also, it Ethereum consumes Ether for any transaction, that is not possible in all situations. Therefore, the technology is still in its early stages, and more research is needed to improve its security and usability for widespread adoption.

### III.2. Proposed System

Our blockchain-based voting system has several security measures in place to ensure the integrity and confidentiality of the voting process. The use of Aadhar number, two times mail OTP, and private key authentication provides a strong form of user authentication to prevent unauthorized access to the voting system. The use of a proof of work algorithm in the blockchain helps to secure the system against malicious attacks, and the merkle tree ensures the integrity of the data even if individual votes are tampered with.

**Advantages:**

We use our own cryptocurrency. So, there is no price amount needed to cast the priceless vote. Safety of your vote can be verified in the telegram bot by entering the vote hash.
IV. Experiments & Results:

Our blockchain-based voting system consists of four main components: the frontend, the blockchain, the backend, and the verification system.

**Frontend:**
The frontend is built using the Django framework and provides a user interface for voters to cast their votes. The frontend includes a login page where users can enter their Aadhar number to authenticate themselves. Once authenticated, the user is directed to the voting page, where they can select their preferred candidate. The voting page includes a list of candidates along with their photos and a brief description of their qualifications. This information is retrieved from the Django administration backend.

**Blockchain:**
The blockchain is the backbone of our system and stores all voting data. We use a proof of work algorithm to secure the blockchain against malicious attacks. Each block in the blockchain contains a merkle tree of all the votes, which ensures the integrity of the data. The blockchain is replicated across multiple nodes to ensure that it is resistant to single-point failures. Each node in the blockchain network is responsible for validating new blocks before adding them to the blockchain.

**Backend:**
The backend is responsible for processing and validating votes. When a user casts their vote, the vote is first authenticated using two times mail OTP and private key authentication. Once authenticated, the vote is added to the blockchain. The backend also includes Django administration, where new users and candidate details can be added. The Django administration backend is accessible only to authorized users and is secured using password authentication.

**Verification System:**
The verification system is responsible for ensuring the integrity of the voting process. We use a Telegram bot to allow users to verify their vote. The bot retrieves the user's vote from the blockchain and compares it to the user's selection on the voting page. If the two match, the vote is considered valid. If not, the user is notified that their vote may have been tampered with. The Telegram bot is also responsible for sending notifications to users when their votes are successfully recorded in the blockchain.

![Blockchain Voting System Diagram]

**Analysis:**
Centralized voting and blockchain voting are two different approaches to conducting elections. Here is a comparison between the two:

Security: Blockchain voting is more secure than centralized voting because it uses advanced encryption techniques to secure the voting data. The blockchain is a decentralized and distributed ledger that records all transactions in a secure and tamper-proof manner. This makes it virtually immutable and resistant to manipulation.
impossible for anyone to hack or manipulate the voting data. Centralized voting, on the other hand, is vulnerable to hacking and manipulation because all the data is stored on a centralized server. 

**Transparency:** Blockchain voting is more transparent than centralized voting because all the transactions are publicly visible on the blockchain. This makes it easy for anyone to verify the accuracy and integrity of the voting data. In centralized voting, the data is controlled by a single entity, making it difficult to ensure transparency.

**Accessibility:** Centralized voting is more accessible than blockchain voting because it does not require any specialized knowledge or equipment to participate. All you need is a ballot and a polling station. Blockchain voting, on the other hand, requires voters to have a computer or smartphone and a basic understanding of blockchain technology.

**Cost:** Blockchain voting is more expensive than centralized voting because it requires a significant amount of computing power and storage space to maintain the blockchain network. Centralized voting, on the other hand, is relatively inexpensive because it uses existing infrastructure and does not require any additional resources.

**Speed:** Centralized voting is faster than blockchain voting because the results can be tallied in real-time. Blockchain voting, on the other hand, requires time to validate and confirm each transaction on the blockchain, which can slow down the process.

**CENTRALIZED VS BLOCKCHAIN SYSTEM**

Overall, blockchain voting is more secure and transparent than centralized voting, but it is less accessible and more expensive. Centralized voting is faster, more accessible, and less expensive, but it is more vulnerable to hacking and manipulation. The choice between the two approaches depends on the specific needs and requirements of the election organizers.
Security:

Security is a critical aspect of any electronic voting system. In our system, we use multiple layers of security to ensure the integrity and confidentiality of the voting process. We use Aadhar number for user authentication, which is a government-issued identity card in India. We also use two times mail OTP and private key authentication to prevent unauthorized access to the voting system. The blockchain is secured using a proof of work algorithm, which makes it difficult for attackers to tamper with the data. The merkle tree ensures that the integrity of the data is maintained even if individual votes are tampered with.

Advantages of Blockchain-Based Voting System:

The proposed blockchain-based voting system has several advantages over traditional voting systems.

- **Security:** The use of blockchain technology provides a secure and tamper-proof voting experience for users. Once a vote is recorded on the blockchain, it becomes immutable and tamper-proof.
- **Transparency:** The use of blockchain technology provides a transparent voting experience for users. Users can verify the integrity of the voting results using the Merkle tree.
- **Accessibility:** The proposed system allows users to cast their vote from anywhere using a web-based interface.
- **Efficiency:** The use of blockchain technology allows for efficient and secure verification of the voting results.
- **Accountability:** The proposed system allows for the creation of a permanent and auditable record of the voting results.

V. Conclusion and Future Work

The proposed blockchain-based voting system offers a secure, transparent, and accessible voting experience for users while addressing the challenges and limitations of traditional voting systems. However, there are still challenges to be addressed, such as scalability, usability, and regulatory compliance. In future work, we plan to address these challenges and further enhance the security and transparency.

References:


