Crypto Vote: Enhancing Electoral Integrity through Blockchain Based Online Voting

Priyanshu Gupta, Punit Mittal, Riya Agarwal, Vikrant Singh
Dept. Computer Science & Information Technology Meerut Institute of Engineering & Technology Meerut, India

***Abstract*— All the conventional voting methods are also associated with various problems such as security issues, lack of transparency, and cases of wrongful voting. This paper proposes a blockchain based voting application that takes advantage of the properties of decentralization, immutability and transparency of the blockchain in order to solve all these problems. This system is implemented with the help of Solidity smart contracts and the easy to use frontend is created using React.js, to meet important voting criteria such as voter qualification, one voter one vote and vote anonymity. With MetaMask for wallet based voter identification and Ethereum for the preservation of transaction history, the system provides a secure, efficient and tamper proof voting system. The proposed method helps in creating the ballot, casting the vote and counting the votes in autonomous manner with high level of transparency and auditability. The test outcomes show that the system is efficient, robust and robust against traditional electoral risks. This research shows the potential of blockchain technology in improving conventional voting processes and provides a foundation for future work to customize the system for actual world implementation.**

Keywords*— *Blockchain Technology, Decentralized Voting, Ethereum, Smart Contracts, E-Voting Systems

I. INTRODUCTION

A. Background

Voting is the cornerstone of democracy, where people are given a chance to register their views and contribute to the decision-making processes. However, conventional voting procedures are associated with various problems such as voter fraud, manipulation, low transparency and slow voting tallying. These issues can erode the public's confidence in the political system, pointing to the need for a voting system that is more secure, more transparent, and more efficient.

B. Role of Blockchain in Modernizing Voting

With blockchain technology, there is a way to have a decentralized, tamper proof and transparent system that can replace the conventional voting methods. The ability of blockchain to record transactions in a secure manner, and the automation of those processes through smart contracts, makes it a perfect fit for building reliable voting systems.

C. Objectives of the Proposed System

This research is aimed at developing a voting system based on blockchain technology for the following goals:

- Secure Authentication: Voters' eligibility is established by verification against a MetaMask wallet.
- One Person, One Vote: Smart contracts can be used to enforce these rules on the blockchain to prevent one voter from casting more than one vote.
- Transparency and Immutability: All votes are made and stored on the blockchain, making the results impossible to alter and easy to verify.
- Automated Vote Counting: Design smart contracts to tally the votes which minimizes human error.

D. Scope of the Research

The system is built on the Ethereum blockchain and consists of:

- Some smart contracts written in Solidity to govern voting and procedures.
- A web application built with React.js, with easy-to-use interface.
- Coupled with MetaMask, a solution for voters to verify their identity and conduct transaction

This research shows how the use of blockchain

technology can improve the credibility and the openness of the voting processes through a secure and decentralized voting system. As for the crucial factors, such as voter qualification, ballot secrecy, and accuracy, the proposed solution demonstrates the possibilities of the blockchain to improve conventional electoral systems.

II. RELATED WORK

A. Blockchain Applications in Voting

Because of its ability to revolutionize voting systems, blockchain technology has drawn a great deal of interest. To streamline electoral processes and ensure that established criteria are met during voting, [1] propose a permissioned blockchain model with smart contracts. Their framework entails district nodes and bootnodes that are run by authorized entities to oversee network connectivity. The decentralized and transparent voting environment that this method offers solves the problems of voter coercion and electoral fraud. However, to meet the very strict privacy and security requirements, it is necessary to operate in somewhat controlled environments.

In the same manner, [4] combined biometric authentication with blockchain technology to safeguard the voting process. Iris recognition is used for voter identification and One Time Password (OTP) methods to ensure that only the qualified voter can vote. The data collected is stored on the blockchain ledger and is irreversible, thus enhancing trust in the process. It, therefore, positions itself as a secure and transparent solution for conducting electoral processes. This research shows how it is possible to combine the new generation of authentication methods with the blockchain to solve some of the critical issues of the traditional systems.

In [7], a decentralized ledger was recommended to guarantee the integrity of voting processes and provide instantaneous results. The approach of the methodology is based on smart contracts for implementing the main voting procedures or casting a vote, or proving your eligibility to vote, or counting the results. Thus, we have minimized the need for human input in the process. Nevertheless, the research uncovered challenges, including scalability and network latency, that still hinder deployment in large-scale elections.

Ref. [9] reviewed the application of enterprise blockchain technologies like Hyperledger for developing permissioned voting systems for institutional elections. Unlike public blockchains, the enterprise solutions are more controlled to improve performance and scalability. Vote automation and validation and counting are being done through smart contracts to increase the level of security and trust. From their study, they concluded that enterprise blockchains are well-positioned to meet the needs of environments that need more control and efficiency, e.g., corporate or governmental elections.

In a thorough review performed by [3], various blockchain voting systems were assessed against the global standard for voting. The research found that the immutability and the transparency of the blockchain are suitable to build confidence into the voting processes. However, the authors of the article pointed out that there are problems of scalability, voter privacy, and legal issues that need further study and improvement.

Moreover, [8] proposed a voting system based on blockchain, which uses homomorphic encryption to preserve voter anonymity and guarantee the sanctity of the vote. They achieve this by encoding the votes on a public blockchain such that no one can change them and at the same time make them verifiable. This protocol shows how cryptographic tools can be used to solve the problem of privacy versus accountability in the context of large elections, although it has some scalability issues.

B. Challenges in Current Blockchain-Based Voting Systems

Despite these benefits however, there are numerous challenges that inhibit the scalability and acceptance of voting systems based on blockchain technology. In his review, 2 highlighted scalability as a main challenge, particularly for national elections that are characterized by high transaction throughputs. He also stressed the need for traditional performance indicators to support the evaluation and improvement of the system. Introducing a method that uses homomorphic encryption to protect voter privacy and store votes securely is a great

idea, but implementing this on a large scale has been a challenge.

Another study, [3] reviewed the use of cryptographic methods and global standards in blockchain enabled e- voting platforms. While blockchain improves security and confidence, there are still some issues regarding voter privacy and compliance with the rules. Likewise, [5] also proposed the use of dual blockchains to address voter anonymity, but the problem of balance between privacy and scalability remained unsolved.

C. Alignment of the Proposed System

The proposed voting system based on blockchain is an improvement on previous research in that it addresses critical problems of scalability, transparency, and secure authentication of voters. The system validates voter eligibility through verification by MetaMask wallets and maintains anonymity. It uses a decentralized ledger to store votes as done in studies cited in [7] and [9] to make the results immune to tampering. Also, the use of smart contracts for vote counting is in line with the automation goals identified in [1] and [8].

This research is intended to provide a real world application of blockchain technology to electoral processes while also meeting the challenges of scalability, voter authentication and user friendliness and supporting the further development of secure and transparent e voting systems.

III. PROPOSED SYSTEM

A. Overview of the System

The proposed voting system based on blockchain improves the credibility of the election process with the help of blockchain technology's immutability, accuracy and accountability. The goal is to create a secure, decentralized and immutable way of casting votes. The primary goals are to guarantee that only eligible voters can cast a vote, that one voter cannot cast more than one vote, that the vote cannot be linked to the voter and that the voting can be counted in real time.

The system design also enhances the process of keeping the data accurate and smooth by incorporating smart contracts, MetaMask wallet authentication and decentralized blockchain storage system. This way, people are able to cast their votes directly in a reliable and transparent environment, without the need of a intermediary third parties.

B. System Components

1) Blockchain Network: This thesis uses a public blockchain, such as Ethereum, to make sure that votes are transparent and permanent. Every vote is considered a transaction that is written to the blockchain for eternity. The decentralized nature of the blockchain makes it nearly impossible to alter or alter votes in any way.

2) Smart contracts: The system's essential functions are automated by smart contracts that form its base. They enforce regulations like the following:

- Voter Eligibility: It confirms the voter's credentials by linking to the MetaMask wallet.
- Vote Casting: Guarantees that every participant's wallet address is saved after successful participation, so that only they can vote once.
- Vote Counting: Automatically calculates the votes instantaneously, eliminating manual mistakes and delays.

3) Voter Authentication using MetaMask: MetaMask wallet is implemented to authenticate the voter. Each voter has to link their wallet to the platform, making it secure and private. This way of identifying who is allowed to vote ensures that only the qualified voters can vote and there is no way of voting in another person's name.

4) Distributed vote storage: The blockchain has encrypted the votes as the transactions, such that no one can know the voters' identities while the blockchain provides the transparency of the vote. In this manner, all sides can verify the tally of the votes without threatening the anonymity of each voter.

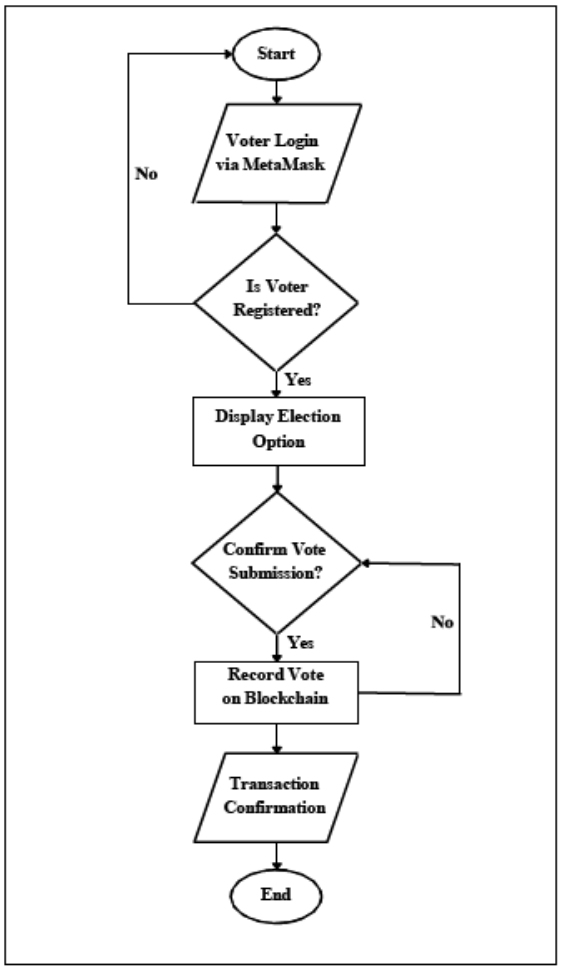

Fig. 1. Voter Function Flowchart.

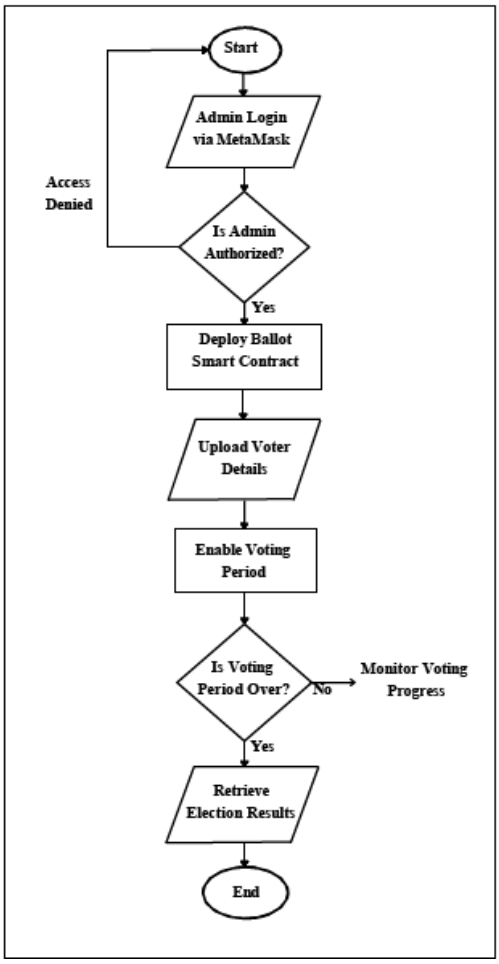

Fig. 2. Admin Function Flowchart

C. Workflow of the System

1) Voter Enrollment: Only registered voters are allowed to vote and for that, they have to enroll their MetaMask wallet on the platform one week before the voting starts. All the registration details are securely saved and verified on the blockchain.

2) Vote Casting: When the election begins, people register their participation using their MetaMask accounts and make their selection of the candidate. The smart contract checks their eligibility and puts their vote on the blockchain. Once submitted, the wallet address of the voter is flagged as 'used' to avoid voting more than once.

3) *Vote Storage and Encryption*: All the votes are recorded as the transaction on the blockchain and the encryption is done to protect the voters' privacy. The unchangeable ledger of the blockchain makes it impossible to alter or delete the votes.

4) *Real-Time Vote Count*: The smart contract casts the votes for you as they come in, quickly and accurately. The results can be obtained from a secure platform, without having to know the votes themselves by election officials and other interested parties.

D. Key Features of the Proposed System

Decentralization: The platform is based on a decentralized blockchain network, there are no central authorities which reduces the risk of fraud or manipulation.

Security & Privacy: The cryptographic votes are securely stored on the blockchain and the voters'

identities are kept anonymous. MetaMask wallets are used to increase the level of security when authenticating users.

Transparency & Trust: Blockchain's immutability makes it possible for all interested parties to check election outcomes for themselves, thus increasing the credibility of the election process.

Scalability: The system was initially developed for small to medium elections and can be enhanced to support large elections through the optimization of smart contracts and the blockchain network.

IV. IMPLEMENTATION AND RESULTS

A. System Development Environment

1) Development tools:

- Truffle Framework: Used to create, test and deploy smart contracts, it is a development environment for blockchain apps.
- Ganache: It is used as a local emulator of the Ethereum blockchain, to test smart contracts and decentralized applications).
- MetaMask: It is a browser extension wallet, that helps with authentication and interaction with the Ethereum network.
- Node.js: It is used to run the server-side components and to manage dependencies.
- React.js: It is used for designing the user interface of the application and is a frontend framework for creating dynamic user interfaces.

2) Programming Languages:

- Solidity: Smart contracts were developed with the help of Solidity, which is the predominant language for the Ethereum blockchain.
- JavaScript: Used for the user interface and to communicate with smart contracts using Web3.js.

3) Smart contracts:

- Migrations.Sol: This contract is utilized to oversee the deployment of other contracts.
- Voting.sol: This is the central contract responsible for voting activities, including ballot creation, vote submission, and result tallying.

B. Results

The proposed voting system utilizing blockchain technology was evaluated with Ganache, a local simulator for the Ethereum blockchain. Ganache offered ten pre- funded accounts with 100 ETH, facilitating straightforward testing of smart contract features. The assessment of gas consumption for crucial system operations resulted in the following findings:

TABLE 1. GAS CONSUMPTION FOR VOTING SYSTEM

Operations	ETH Consumed	Gas Consumed
Ballot Creation	0.00364587 ETH	1446214
Add Voters	0.00018635 ETH	73996
Create Choices	0.00019131 ETH	76068
Start Voting	0.00011723 ETH	46648
Cast Vote	0.0002976 ETH	118490
End Voting	0.00014282 ETH	56896

V. DISCUSSION AND ANALYSIS

A. Analysis of Gas Consumption

Table 1 presents the gas usage for essential functions in the blockchain-based voting system. The operation of Ballot Creation consumed the most gas, totaling 1,446,214 gas units. This is anticipated since this process involves deploying a new contract with comprehensive voting settings, making it computationally demanding.

Conversely, functions like Add Voters (73,996 gas) and Start Voting (46,648 gas) require substantially less gas, as they mainly involve simple data storage and transitions in state.

The Cast Vote action, which consumes 118,490 gas, reflects the expense of securely logging individual votes and modifying the smart contract's state. This is essential for preserving the integrity and immutability of the voting process.

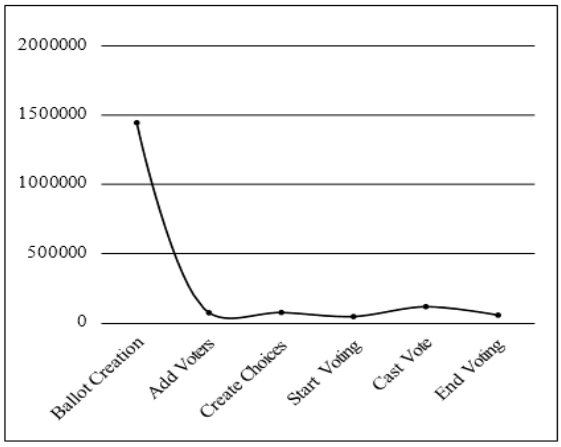

Fig. 3. Gas Consumption for System Function.

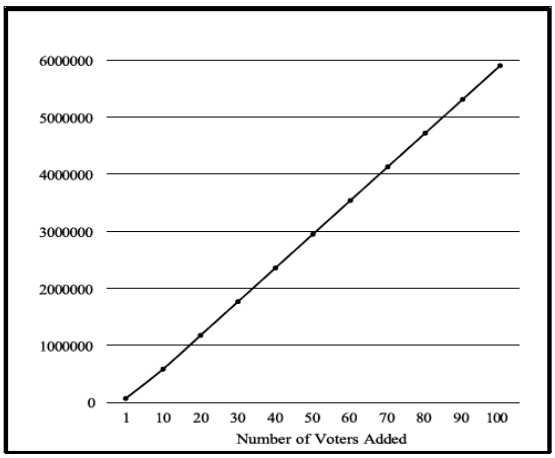

Fig. 4. Gas Consumption for Adding Voters

B. Comparison with Existing Systems

The performance of this system was compared to similar blockchain-based voting solutions documented in the literature:

- Ref. [1] proposed system utilized permissioned blockchains, which resulted in gas-efficient operations but limited scalability for public use. In comparison, our system, based on Ethereum, provides decentralized transparency while maintaining moderate gas efficiency.
- Ref. [8] e-voting protocol used homomorphic encryption for voter privacy, which significantly increased gas consumption during vote tallying. Our system achieves comparable privacy while reducing gas costs for core operations.
- The meta-analysis of [2] highlights that gas optimization and scalability are critical for large-scale adoption. Our system's gas usage aligns with the benchmarks they reported for small-to-medium scale voting applications.

C. Significance of Results

The findings indicate that the proposed system maintains a good balance between transparency, security, and efficiency in resource use. The measurements of gas consumption imply that it is well-suited for municipal or organizational elections where the number of voters is manageable. Further enhancements for national elections, including Layer-2 scaling solutions or zero-knowledge proofs, could boost efficiency and reduce costs.

By incorporating effective strategies from current systems, including the implementation of smart contracts for automation and a permissionless blockchain for transparency, this project provides a scalable framework. Future endeavors may investigate enhancements in scalability and cryptographic privacy methods to improve competitiveness with new emerging solutions.

TABLE 2. COMPARISON OF PROPOSED, TRADITIONAL AND EXISTING BLOCKCHAIN VOTING SYSTEM

Feature	Proposed System (Your Project)	Traditional Voting System	Existing Blockchain Voting Systems
Security	High (Blockchain with Smart Contracts)	Low (Prone to Tampering)	High, but limited in voter privacy
Transparency	High (Public Ledger)	Low	High
Voter Anonymity	Maintained through Wallet Address	No	Partial (Depends on Encryption Tech)
System Cost	Low (Decentralized System)	High (Printing and Infrastructure)	Moderate (Gas Fees on Public Blockchain)
Vote Manipulation	Impossible	Possible	Impossible

Scalability	Suitable for Small to Medium Elections	Suitable for Large Elections	Low (High Gas Consumption)
Result Time	Instant	Delayed	Instant

VI. CONCLUSION

This research paper outlines the development and execution of a voting system that uses blockchain technology, specifically utilizing Ethereum smart contracts to provide transparency, security, and decentralization throughout the electoral process. The system underwent thorough testing with Ganache, and the findings show its effectiveness regarding gas usage for different functions like creating ballots, registering voters, and casting votes.

In contrast to conventional and current blockchain voting solutions, the suggested system provides major benefits, such as automated workflows, secure vote documentation, and instant result calculation, all while ensuring computational effectiveness. The analysis of gas consumption validates the system's feasibility for elections of small to medium sizes.

Even with its promise, the system confronts obstacles in scaling for a nationwide rollout, which may be tackled through future improvements like Layer-2 scaling approaches or sophisticated cryptographic methods such as zero-knowledge proofs.

In summary, the suggested voting system utilizing blockchain technology reveals a practical method for updating electoral procedures, adding to the expanding research focused on improving trust, transparency, and efficiency in democratic systems.

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to everyone who contributed to the completion of this review paper. My sincere thanks go to my mentors and advisors, whose guidance and valuable insights were instrumental throughout the research process. I am especially grateful to the authors of the research papers referenced in this study, whose work laid the foundation for this comprehensive research.

Additionally, I wish to thank my peers and colleagues for their constructive feedback and encouragement, which inspired me to refine and enhance my work. Finally, I acknowledge the support of my institution and the resources provided, which enabled me to carry out this research successfully.

REFERENCES

[1] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 983–986. doi:10.1109/CLOUD.2018.00151

[2] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, ‘A systematic literature review and meta-analysis on scalable Blockchain-based electronic voting systems’, *Sensors (Basel)*, vol. 22, no. 19, p. 7585, Oct. 2022.

[3] Y. Abuidris, R. Kumar, and W. Wenyong, ‘A Survey of Blockchain Based on E-voting Systems’, in *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, Xi’an, China, 2020, pp. 99–104.

[4] Pawade, D., Sakhapara, A., Badgujar, A., Adepu, D., & Andrade, M. (2020). Secure Online Voting System Using Biometric and Blockchain. In N. Sharma, A. Chakrabarti, & V. E. Balas (Eds.), *Data Management, Analytics and Innovation* (pp. 93–110). Singapore: Springer Singapore.

[5] Kumar, D. Dwijesh, et al. "Secure electronic voting system using blockchain technology." International Journal of Smart Home 14.2 (2020): 31-38.

[6] Patil, Harsha V., Kanchan G. Rathi, and Malati V. Tribhuwan. "A study on decentralized e-voting system using blockchain technology." Int. Res. J. Eng. Technol 5.11 (2018)

[7] Shah, Akhil, et al. "Blockchain enabled online-voting system." ITM Web of Conferences. Vol. 32. EDP Sciences, 2020.

[8] Liu, Yi, and Qi Wang. "An e-voting protocol based on blockchain." Cryptology ePrint Archive (2017).

[9] Denis González, Camilo, et al. "Electronic voting system using an enterprise blockchain." Applied Sciences 12.2 (2022)