International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

Decentralized Voting System Using Blockchain

Prachi Agarwal[1], Ishit Tyagi, Manya Bhardwaj, Abhit Kumar, Aditi Veniwal

1Assistant professor, Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad, U. P., India

reachtoprachi@gmail.com, tishit705@gmail.com, manyabhardwaj954@gmail.com, kumarabhit981@gmail.com, aditiveniwal254@gmail.com

ABSTRACT

The need for trustworthy elections is a cornerstone of democratic governments, yet traditional voting systems and electronic centralized solutions are prone to problems that include but are not limited to: opacity, tampering vulnerability, delayed processing of results and reliance on trusted institutions. These constraints erode the credence of election results with the public. In this paper, we are going to present a decentralized voting system by utilizing blockchain technology to fix such problems. We introduced a system that is built on the Ethereum blockchain, applying smart contracts to provide secure, transparent, and immutable voting process. Every vote is a permanent blockchain transaction, impossible to corrupt or tamper with. Features include wallet-based authentication, automated vote tallying and verifiable results. The proposed solution consistently provides trust, security and transparency to authorities who are conducting the elections and is appropriate for small scale as well as medium size of elections.

1. INTRODUCTION

Voting is one of the most important things in a democratic system, which gives the people the power to decide directly by choosing their leaders. In order for the electoral procedure to be trusted, it should guarantee transparency, security, fairness plus voter privacy. However, the traditional voting instruments like paper ballots and electronic voting machines that are done in the same centralized place have many issues such as vote tampering, lack of transparency, slow result processing, and dependence on centralized authorities.

The idea behind internet voting together with centralized electronic voting was to make the whole process more accessible and efficient. Nevertheless, these systems are still open to cyber, attacks, threats from insiders, unauthorized access, and data manipulation. Also, as the whole election infrastructure is in the hands of a single entity, the voters have to trust intermediaries blindly, which usually results in low trust in election results. There is still a tough problem in ensuring the privacy of voters while the results are verifiable and there is no chance for tampering.

As a result, blockchain technology has been identified as a potential candidate to remove the obstacles. Blockchain is a decentralized and distributed ledger that records the transactions in the most transparent and permanent way. The main features of the technology, decentralization, cryptographic security, immutability, and consensus mechanisms, remove single points of failure and make it possible for independent verification of the data recorded.

Blockchain has the features that make it an ideal technology for constructing secured systems. To address the problems of security and trust that exist in traditional and centralized voting systems, this article presents a decentralized voting system utilizing blockchain technology. By using smart contracts, the proposed system automates voter authentication, voting, and obtaining the final results in a secure and transparent way. Each vote is a transaction on the blockchain that cannot be altered, thus ensuring that the data is accurate, the voters are anonymous, and anyone can check the correctness of the results.

The main goal of this study is to create a voting system that is safe, transparent, and trustworthy, thus leading to an increased level of trust in the electoral process without the need for centralized control.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

2. RELATED WORKS

Various research initiatives have delved into the application of blockchain technology to make voting systems more secure and transparent.

[1] designed a decentralized electronic voting mechanism powered by the Ethereum blockchain to do away with centralized authority. Even though the operation makes the system more open and unchangeable, it still lacks sufficient privacy of the voters because the ballots can be traced in the course of voting.

[2] presented a voting system utilizing blockchain technology that uses biometrics for voter verification. Even though the technique solidifies voter authentication, it still relies on several trusted third parties, which lowers the overall decentralization degree. [3] came up with a smart contract, based on a voting mechanism with different contracts for voter registration and election management. Nonetheless, the device complicates the situation further and causes privacy and scalability issues to be of concern.

[4] introduced a voting framework enabled by the blockchain that integrates biometric verification and cryptographic hashing for better vote integrity. However, the privacy of users needs to be guaranteed more strongly and the system should be more transparent in order to get the trust of the voters. [5] created the Bronco vote, a voting system based on blockchain, aimed at university elections mainly. Although it makes the process transparent and easy to audit, the platform has weak voter registration methods and limited authentication security.

[6] presented a blockchain, based electronic voting system architecture with the use of smart contracts to provide features like anonymity, integrity, and transparency. Even though the technology enhances election security, it has issues concerning scalability and transaction fees. In general, the existing blockchain voting systems show the promise of decentralized technology but still have some problems like privacy concerns, high operational costs, scalability problems, and partial dependence on certain parties.

The system that is being proposed intends to fill in these voids by providing a decentralised voting solution that is secure, privacy preserving and cost efficient.

3. PROPOSED METHODOLOGY

In this section, the proposed approach for designing and implementing a distributed voting system based on blockchain technology shall be discussed. The main aim of this approach is to provide security, transparency, anonymity, vote integrity, and trustless verification to eliminate the need for intermediaries. In a general architecture, voting systems based on blockchain technology rely on a blockchain network and smart contracts governed by external bodies.

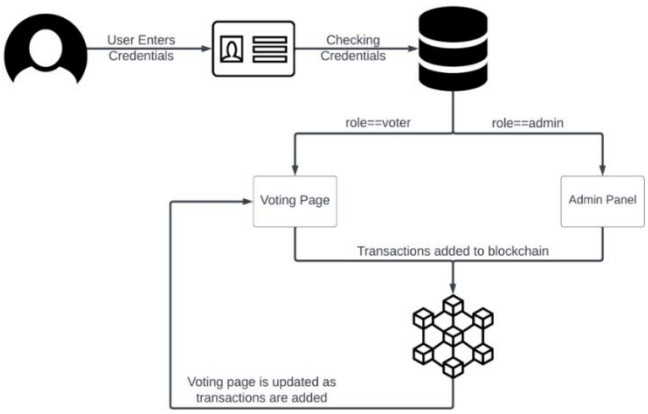

Fig 1: System Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

3.1 System Architecture Overview

The proposed system employs a Decentralized architecture where every voting activity has been recorded on a blockchain. The blockchain can be viewed as a Distributed Database that records every single Vote as a cryptographically secured transaction on the blockchain. It utilizes Smart Contracts on the blockchain that automatically implement the rules governing elections.

The system has the following main entities:

- Election Commission (EC)
- Voters
- Candidates
- Blockchain Network
- Smart Contracts Each of these entities has roles and permissions that enable engagement with the election system to ensure equity and security.

3.2 Election commission module

In the context of the Indian elections, the Election Commission (EC) is trusted for overseeing the entire process of elections. It is not responsible for controlling the votes.

Some of its duties include:

- Carrying out a new election
- Voters and Candidates Registration
- Setting up election parameters like start time, end time, and list of candidates
- Deploying smart contracts on the blockchain
- Closing the election after the stipulated time

Once the election process is triggered by activation, no changes to votes or results are possible by the EC. This promotes decentralization and integrity.

3.3 Voter Registration and Authentication

In general Voters who are eligible to vote get registered by the Election Commission prior to the commencement of the election. Each voter gets a unique blockchain identity, also referred to as a public key.

Authentication is made possible by the use of cryptographic methods

- Public-private key pairs
- Digital signatures

During the login process, the voters verify themselves using their private keys to ensure that only authorized voters access the voting system and that no voter tries to impersonate another voter.

3.4 Moule for Registration of Candidates

The Election Commission registers the candidates before the election. Every candidate has an id and is stored on the blockchain via smart contract.

Candidate information is immutable once registered, meaning it can't be manipulated once it's been deployed.

3.5 Smart Contract Design

The core of the proposed methodology will be based on smart contracts. The main task of this method is the automatic enforcement of election rules. Among the major functions of the smart contract are:

Electoral roll verification is used in five democracies:

To determine the eligibility of voters.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

- Double Voting Prevention
- Secure vote recording
- Maintaining anonymity of voters
- Counting the votes transparently

It is coded in such a way that the smart contract can ensure each voter voted once, and once votes are recorded onto the blockchain, they will remain there in perpetuity.

3.6 Vote Casting Process

Procedure followed in the vote-casting steps are as follows:

- The voter logs in to the system utilizing their blockchain credentials.
- It checks the eligibility of voters through the smart contract.
- The voter chooses a candidate.
- The vote is encrypted and sent as a transaction in the blockchain.
- It involves the validation and registration of the vote on the blockchain.

Once the vote has been submitted, it cannot be edited or deleted. This ensures immutability.

3.7 Anonymity & Privacy Preservation

Anonymity in voting can be accomplished by decoupling voter identity from voting data. The voting system does not record any private data on the blockchain network. Vote data can only be tracked using anonymous public keys, thereby making it computationally infeasible to trace a vote to an individual voter. Other methods of cryptography, like hash functions and encryption, are also used for additional security of voter privacy.

3.8 Result Generation and Verification

Following the election period, the smart contract automatically disables the casting of votes. The counting of the votes is done transparently in the smart contract system.

Because all votes are visible on the blockchain, vote results will be independently verifiable by any voter without disclosing their identities. This is what will promote transparency, trust, and auditability outcomes.

3.9 Security Considerations

“The proposed methodology deals with the common security threats in the following ways:”

- Decentralized systems that remove single points of failure.
- Immutable blockchain to ensure votes are not manipulated
- Smart contract audit to avoid vulnerabilities
- Authentication using cryptographic techniques to protect against unauthorized access

These measures, taken together, work towards making the voting process more reliable.

3.10 Workflow Summary

Overall workflow is summarised as follows:

- The Election Commission launches the election smart contract
- Voters and candidates are registered
- Election is activated
- Votes are cast using cryptography
- The votes are verified and logged on the blockchain
- Election is closed
- Results are automatically generated and verified

This new methodology guarantees a safe, transparent, and secure voting system suitable for modern electronic elections.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

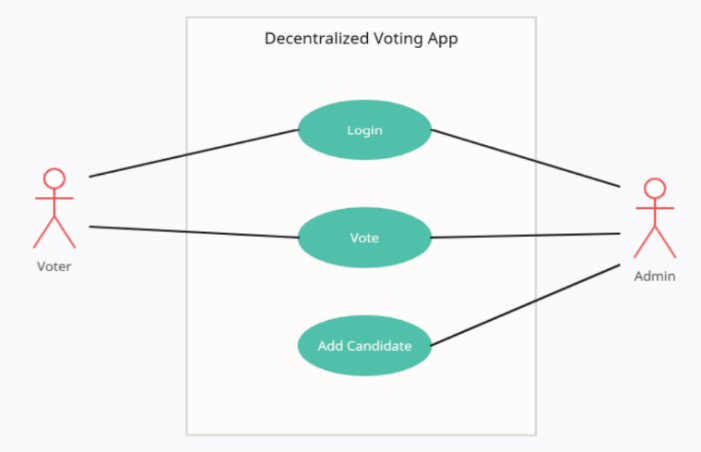

Fig 2: Use Case Diagram

4. IMPLEMENTATION

The Ethereum blockchain technology is a promising option for computerized voting applications. The Ethereum blockchain provides the ability to design smart contracts. The term" smart contract" refers to a computer program or transaction protocol designed to automatically perform appropriate activities according to the conditions of the agreement. Smart contracts have many objectives, including the elimination of trusted intermediaries, the reduction of arbitration and enforcement costs, the reduction of fraud losses, and the elimination of intentional and inadvertent exceptions. There are two kinds of accounts supported by Ethereum. An externally owned account (also known as a user-controlled account) is controlled by a user. These accounts are denoted by the letters EOA. A contract account is managed by the smart contract that is running on the computer. A contract account is denoted by the letter CA. Both kinds of accounts are capable of storing the Ethereum cryptocurrency, or ether. Ethereum does not execute operations (computations) in a smart contract without user input. As a result, before its functions may be performed, a CA must be enabled by an EOA. The EOA must buy 'gas' in order to carry out its operations, and this must be done using the ether currency.

To develop a decentralized application that can effectively substitute a traditional voting system, a website is needed that provides the voting environment. Also, people who cannot go to their polling locations for various reasons may vote by visiting a user-friendly online website displaying their city's election ballot. First and foremost, to implement a blockchain-based voting system in Ethereum, we must first create the necessary environment. The implementation details are shown in Fig.4. The application is divided into basically two sides:

1. Server-side and
2. Client-side

5.1. Server-side

On the server side, there is running a blockchain network. The server-side components are:

1. Truffle
2. Solidity
3. Ganache
4. Node Server

5.1.1. Truffle

Truffle is a solidity programming language-based tool for developing Ethereum blockchains. Truffle also includes features like as automation testing, client-side development, network management, and smart contract administration [7]. The proposed system uses Truffle to manage the network. Truffle is mainly responsible for compiling smart contracts written by solidity, performing migration on various contracts, and generating ABI (Application Binary Interface).

5.1.2. Solidity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

Smart contracts are created utilizing Solidity which is a high-level programming language that is contract-oriented [8]. The functionality of Solidity directly parallels that of JavaScript [9] When utilizing Solidity to create smart contracts developers can structure their contracts in the same method, they would structure classes when using Object-Oriented Programming. Additionally, like most programming languages, the code used to implement smart contracts will be composed of both variable declarations and method definitions [10]. Finally, Solidity uses an intermediate representation called Bytecode that can be run via a compiler on the Ethereum Virtual Machine (EVM) [8].

5.1.3. Ganache

Another tool named ganache is the one that is used for local machine application management and testing. It is a particular RPCServer that can be checked and developed for Truffle, which is available as a mobile and command line application [1]. Ganache usage can be done at any stage of the development process, which makes it possible for dApp to be updated, reused, and tested safely and securely. It is a tool that can run Blockchain locally and do the testing, command issuing, and Blockchain status observing. It's a blockchain simulator that has been installed locally. Ganache employs the graphical interface for Blockchain networks simulation and Smart Contracts live testing without the need for virtual test networks or a remote network [11]. It brings with it the offering of ten pre-funded accounts with 100 Ether each and a 12-word seeds term for the regeneration of such accounts [1].

5.1.4. Node Server

Our system makes use of a minor node server. It serves as a cryptographic server, thereby referred to as a crypto server. The server is responsible for the storage of the public and private keys for encryption and decryption, respectively, as illustrated in Fig. 4. The EC (Election Commission) generates the keys in this server that are employed to secure the votes being cast and then to unveil them at the time of counting.

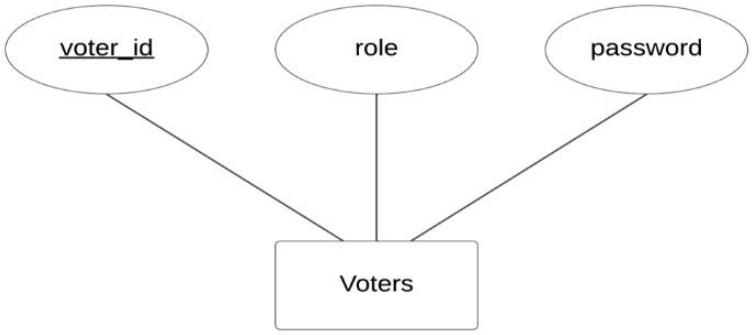

Fig 3: ER Diagram

5.2. Client-side

The Ethereum account holder interface (UI) is the web application developed to allow individuals to cast their votes via an Ethereum account from any computer or mobile device. Several different tools are being used on the client-side to manage the UI, including CSS, which helps with enhance the aesthetic of the design and React JS, for managing all data that is handled by the client-side application. HTML is also used as markup language for this application.

Meta Mask serves as a secure crypto wallet that supports Ethereum wallets for storing Ether (the cryptocurrency created by Ethereum) and allows users to send and receive Ether via decentralized apps (or "DApps") of their choice. As it operates as a lightweight browser extension, it is compatible with many different web browsers, including Chrome, Firefox, Opera and Brave [12].

The public and private keys associated with Ethereal accounts are stored in a Meta Mask wallet, with private keys being used for signing/confirming transactions. Meta Mask has been designed so that its encrypted keys are kept only within the browser, making them less vulnerable to hacking incidents than traditional crypto wallets. Therefore, if hackers were to steal keys from a Meta Mask wallet, there would be no financial loss due to this hack [13]. Meta Mask stores the user's account information, including their balance and both public/private keys. Therefore, it can be thought of as acting as an intermediary between a web browser and a blockchain (or crytocurrecy) network. Meta Mask provides an interface that allows users to make requests of blockchain networks and manage their various coin balances across multiple blockchains/update their account balances.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

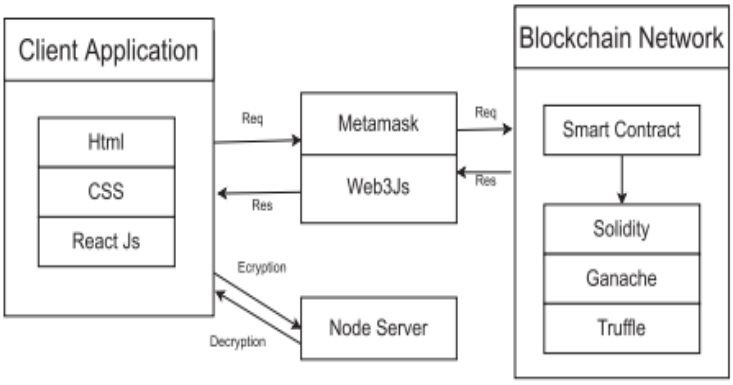

Fig 4: Flow Of Implementation

5.3 System User Interface

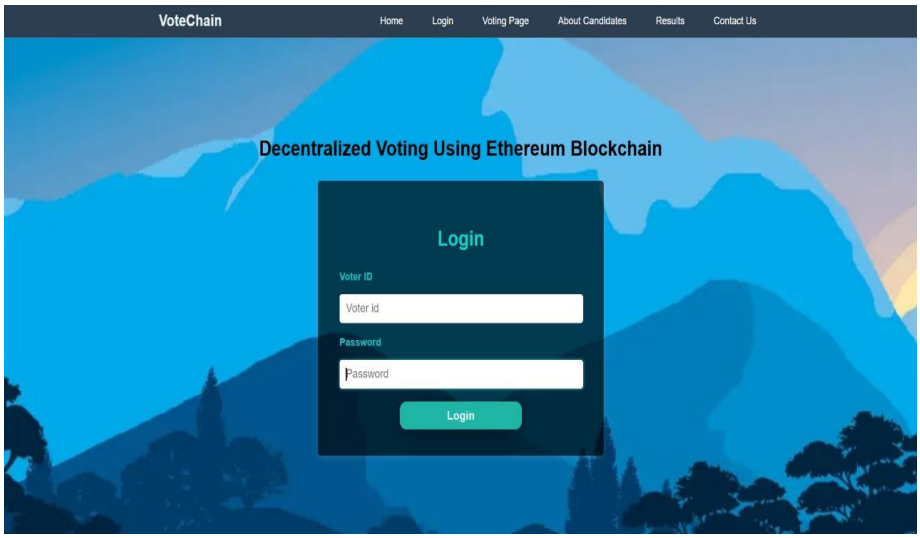

Fig 5: Voter Login Interface

Figure 5 shows the login interface of the decentralized voting system. Registered voters authenticate themselves using their voter ID and password before accessing the voting dashboard.

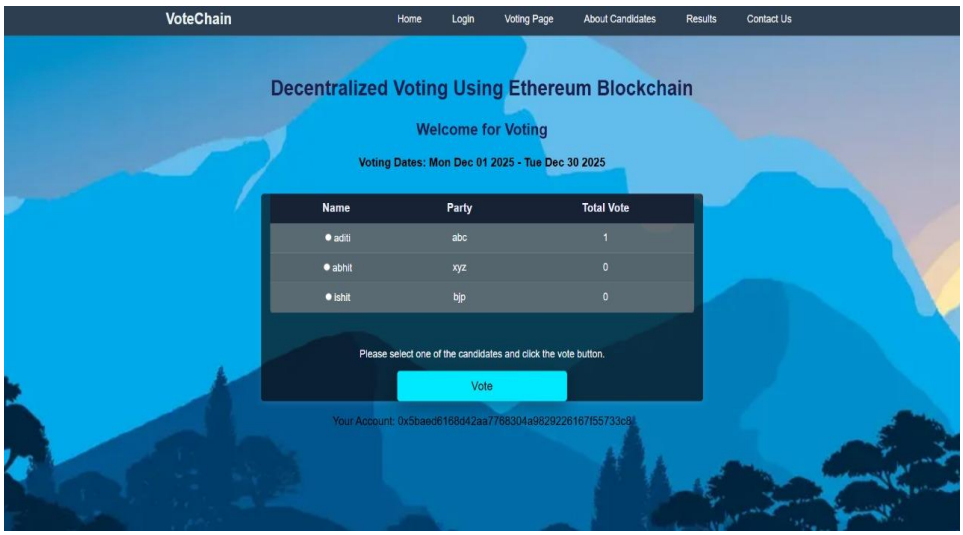

Fig 6: Voting Interface Showing Candidates and Vote Count

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

After successful authentication, voters are redirected to the voting page as shown in Figure 6. The interface displays the list of candidates along with their respective parties. The voter can select a candidate and cast a vote, which is recorded as a transaction on the Ethereum blockchain.

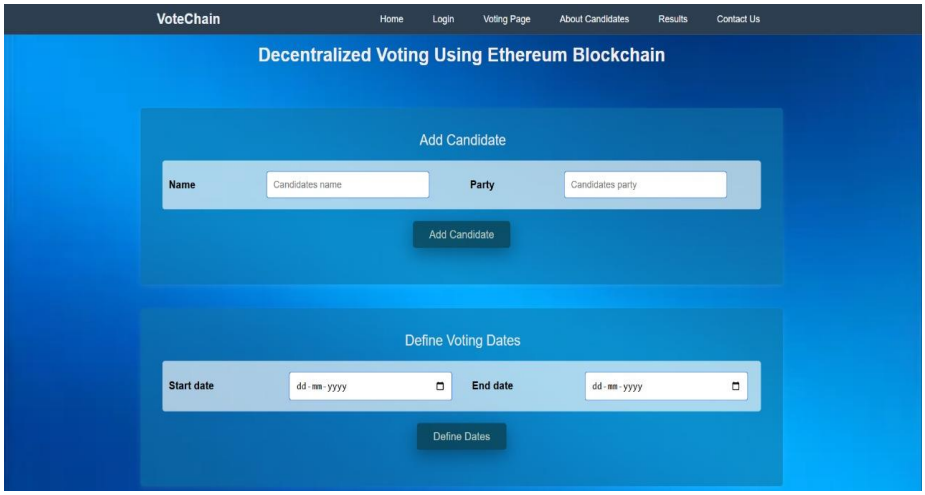

Fig. 7: Admin Dashboard for Candidate Registration and Election Scheduling

Figure 7 illustrates the admin dashboard used by the Election Commission. The administrator can add candidates and define the election start and end dates. Once the election is activated, these parameters become immutable.

5. SECURITY PROPERTY ANALYSIS

In this section, an analysis of the security features offered by the proposed voting system will be undertaken to show how the blockchain technology and cryptography work in unison towards ensuring a secure voting process. The voting process is expected to meet the fundamental security needs required in a modern voting process.

5.1 Anonymity

Anonymity in voting is an important aspect to consider in any voting process to protect the voter from intimidation and guarantee freedom of speech. In the proposed voting system, a voter's identity is not associated with the vote he casts. Every voter communicates with the blockchain system using a distinct public key that acts as a pseudonym.

The vote is recorded in a blockchain transaction, but personal details are not stored. As a result of the encryption that separates a vote or a voter from vote details, a person or adversary cannot trace a vote back to a specific voter because anonymity is ensured while still providing verifiability.

5.2 Privacy

The proposed system ensures the privacy of the voter by ensuring that any secret information of the voter is not revealed before or after the election process.

5.3 Integrity

Vote integrity is responsible for ensuring votes cannot be manipulated or deleted after being cast. In the proposed voting solution, every vote is recorded as a blockchain transaction. As a result of the properties associated with blockchain technology, for instance, hash cryptography and blocks chaining, vote manipulation would be detected instantly.

The smart contracts are responsible for the enforcement of the election rules, ensuring that no recorded vote gets altered throughout the election period.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

5.4 Authentication and Authorization

The system also ensures that only voters who are eligible take part in the elections. The voter verification process is managed through public-private key cryptography, where voters sign all voting transactions digitally.

Smart contracts check for voting eligibility before accepting a vote and also prevent unauthorized persons from voting. Authentication techniques also ensure administrative privileges are not misused, even by the Election Commission, after the start of the election process with respect to voting.

5.5 Non repudiation

Non-repudiation prevents the voter from denying the casting of the vote, and at the same time, it provides for an anonymous process.

5.6 Resistance to Double Voting

The proposed system uses smart contract logic, which eliminates the problem of voting twice. After casting a vote, the smart contract changes the voter information on the blockchain, making it impossible for the same public key to vote again.

Any further voting by the same voter will automatically be disqualified to ensure that the principle of “one voter, one vote” applies.

5.7 Transparency and Verifiability

Transparency can be achieved by keeping a public blockchain ledger where all the voting transactions take place. Although votes themselves are secret, the transaction details can be viewed by all parties.

It means that every stakeholder can independently check for themselves whether or not the voting process and results have been done correctly through an audit of the blockchain.

5.8 Availability and Fault Tolerance

Because it is a decentralized system, the proposed one will not have the problem of single points of failure found in other systems. The blockchain will remain replicated on different nodes to remain accessible in case some nodes fail to perform their operations due to loss of cryptocurrencies on nodes that are compromised by hackers.

This type of fault tolerance ensures that the electoral process has a functioning and trustworthy vote-taking system at all times.

5.9 Opposition to Attacks

This system will be secure against attacks such as vote tampering, repeater attacks, and illegitimate access. Cryptographic authentication, immutable storage, and decentralized consensus make this system resilient to malicious behavior.

Routine audited smart contract coding lessens vulnerabilities, hence improving system security.

In short, the proposed system for a decentralized voting process meets the most important guarantees of security, including the attributes of anonymity, privacy, integrity, and authentication along with the other guarantees of security. It provides the most desirable solution to a secure electronic election process.

6. Conclusions and Future Work

This section concludes the research work by summarizing the proposed decentralized voting mechanism, identifying its current limitations, and highlighting possible directions for future enhancement.

6.1 Summary of the Proposed System

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

In this project, a decentralized voting system using blockchain technology has been designed and implemented to address major challenges present in traditional and centralized electronic voting systems, such as lack of transparency, risk of vote manipulation, single point of failure, and limited voter trust.

The proposed system leverages blockchain and smart contracts to automate and secure the entire election process. Modules such as Authentication & User Management, Admin Dashboard, Candidate Management, Voter Management, Voting & Ballot Module, and Results & Report Module collectively ensure a smooth and reliable voting workflow. Each vote is recorded as an immutable transaction on the blockchain, ensuring transparency and tamper resistance.

To preserve voter privacy, sensitive voter information is handled securely, and each voter is allowed to cast only one vote through smart contract validation. The decentralized nature of the system reduces reliance on third-party authorities and increases trust among participants. Additionally, real-time result generation and auditability make the system more efficient and verifiable.

Overall, the proposed blockchain-based voting system demonstrates that decentralized technology can provide security, integrity, transparency, anonymity, fairness, and verifiability, making it a viable alternative to conventional voting mechanisms.

6.2 Limitations of the System

The current system has some things about it but it also has some limitations. It does not have things like a one-time password or biometric verification to check voter identity, which would make the voter identity verification process stronger.

The voting transactions are stored on the blockchain, which makes each transaction more expensive and can cause problems when a lot of people are voting, like in a big election with many voters. The voter identity verification process would be more secure if the system had -factor authentication mechanisms such, as one time password or biometric verification.

Another limitation is the dependency on users having access to compatible devices and basic knowledge of digital wallets, which may restrict adoption in certain regions.

6.3 Future Work and Enhancements

The future enhancements are going to deal with the problems that were found and make the system work better for people and be easier to use. The system can be made better by adding OTP-based or biometric authentication to make sure the voters are who they say they are. To make the system cheaper to run and faster we can use sidechains or Layer-2 solutions to store the votes somewhere else not on the main blockchain and only keep the final results, on the blockchain. This way the system will be able to handle voters and be more efficient.

Additional features such as mobile application support, multilingual interfaces, advanced analytics, and AI-based fraud detection can also be incorporated. With these improvements, the system can be scaled for national-level elections and adapted for use in universities, organizations, and corporate governance.

Funding

This project did not receive any financial support from public, commercial, or non-profit funding agencies.

Declaration of Competing Interest

The authors declare that there are no competing financial or personal interests that could have influenced the outcomes of this research.

7. REFERENCES

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 04, ICTEM 2.0 (2026)

[1] M. Khan, T. Ahmad, and S. Khan, "Blockchain-based electronic voting system using Ethereum," *Journal of Information Security*, vol. 11, no. 2, pp. 67–75, 2020.
[2] M. Bosri, A. Ahmad, and S. Rahman, "Blockchain-based voting system," *Procedia Computer Science*, vol. 163, pp. 542–549, 2019.
[3] J. Lopes, "Smart contract-based electronic voting system," Master's thesis, University of Lisbon, Portugal, 2019.
[4] B. Shahzad, A. Khan, and R. Malik, "Trustworthy electronic voting system using blockchain," *International Journal of Advanced Research in Computer Science*, vol. 10, no. 4, pp. 15–22, 2019.
[5] G. G. Dagher, P. Marella, M. Milojkovic, and J. Mohler, "BroncoVote: Secure voting system using blockchain technology," in *Proc. IEEE Int. Conf. on Blockchain*, 2018, pp. 96–103.
[6] S. Alvi, I. ul Haq, M. Shafique, and Z. Nawaz, "A secure blockchain-based electronic voting system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 6, pp. 152–159, 2020.
[7] S. Shakya, A. Pandey, and R. Thapa, "Truffle framework for Ethereum-based decentralized application development," *Journal of Web Engineering*, vol. 21, no. 1, pp. 88–95, 2022.
[8] A. Khalid, "Solidity smart contract development for Ethereum blockchain," *Blockchain Journal*, vol. 3, no. 1, pp. 22–29, 2020.
[9] S. Kudva, M. Rao, and P. Shetty, "Solidity programming concepts for decentralized applications," *International Journal of Computer Applications*, vol. 176, no. 29, pp. 12–16, 2020.
[10] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the Ethereum ecosystem," *IEEE Software*, vol. 35, no. 2, pp. 90–97, 2018.
[11] R. Gautam, V. Singh, and A. Kumar, "Blockchain simulation and testing using Ganache," *Journal of Emerging Technologies*, vol. 7, no. 1, pp. 12–18, 2021.
[12] R. Bhavani, P. Kumar, and S. Rao, "Security analysis of MetaMask wallet for decentralized applications," *Journal of Blockchain Technology*, vol. 5, no. 2, pp. 45–52, 2022.
[13] *The Defiant*, "MetaMask security overview," 2022.