IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 10, April 2025

Impact Factor: 7.67

Implementation and Security of Blockchain based Electronic Voting System

Prof. Nasheet Tarik, Mr. Jagda Mohammed Irfan, Ms. Khan Muskaan Firdaus
Ms. Khan Sana Khanum, Mr. Shaikh Mohammed Hassaan
Dept. of CSE (AIML)
M.H. Saboo Siddik College of Engineering, Mumbai, India
nasheet.tarik@mhssce.ac.in, mohammed.2227066.cs@mhssce.ac.in, muskaan.24.khan@gmail.com
sanakhanum2277@gmail.com, hassaan.shaikh825@gmail.com

Abstract: *With increasing demand for a secure, transparent, and efficient election process, blockchain technology has proven to be a promising solution for modernizing the electoral system. This article presents the design and implementation of a blockchain-based E-voting system, using intelligent contracts and distributed networks to ensure data integrity, voter anonymity, and operational prevention interactions. The proposed system allows authenticated administrators to manage elections by adding, updating, or deleting candidates. The investigation begin,s and the results are declared. This allows verified voters to safely hand over their voices and access real results. All voting transactions are recorded on the undercut blockchain, encouraging full transparency and testing potential. Using smart contracts automates polling logic, enforces rules, and minimizes the risk of human error and operations. The paper examines the architecture, interaction and security features of systems and demonstrates the potential to improve the reliability and efficiency of the election process.*

Keywords: Blockchain, E-voting system, Smart contracts, Decentralization, Security, Transparency, Electoral Integrity

I. INTRODUCTION

The sensitivity and disadvantages of the traditional voting systems have demonstrated the urgent need for safer, transparent, and efficient alternatives to maintain the integrity of the election process. Due to its decentralized and tamper-proof nature, blockchain technology has provided a robust solution to these challenges by tackling issues such as voting manipulation, voting fraud, lack of transparency, and operational risk. Our system allows us to register safely, manage (add, update and delete) and declare results of our investigation. In the meantime, voters were able to authenticate themselves, view candidate lists have access to election results in a safe and transparent environment. Integrating blockchain into the voting system was a major advance in overcoming the limitations of traditional election mechanisms, ultimately providing a more reliable, secure, and accessible platform, improving public confidence in the election process.

II. RELATED WORK

The growing interest in leveraging blockchain technology for the electoral process is evident in recent research and implementations. While existing models and conceptual studies have laid a solid foundation, continuous innovation is essential to overcome current limitations and improve voter trust, security, and participation in the

Over the years, the advancements in this field are noteworthy:

Abdulatif et al. (IEEE Member) introduced a blockchain-based voting mechanism utilizing smart contracts. To mitigate the high cost of data storage on the blockchain, the authors incorporate the interplanetary file system (IPFS) for decentralized and efficient data handling. Additionally, the integration of 5G wireless technology enhanced the system

DOI: 10.48175/IJARSCT-25618

performance by offering low latency, high availability, and reliable communication, ultimately resulting in a faster and more seamless voting experience [4]

Pavan M.et al. proposed a solution that integrates blockchain into an existing online voting framework, enabling citizens to vote remotely from anywhere in the world. By storing votes on the blockchain, the system ensures tamper-resistance and data integrity, eliminating the need for physical queuing and reducing the administrative burden on election authorities. The architecture comprises two modules: one for the Election communication to handle candidate registration and election creation, and another for voters to access election details and cast their votes. However, limitations include the system's inability to operate on the Ethereum mainnet, the need for an external Web3 provider, and the absence of a public APL for voter ID verification, posing challenges for voter authentication [5].

Suman Majumdar et al. introduced the ECC-EXONYM e - Voting protocol, built on a decentralized service-oriented architecture using the Exonum private blockchain. The protocol leverages elliptic curve cryptography (ECC) and a hybrid consensus mechanism combining practical Byzantine Fault Tolerance (PBFT) and RAFT. It employs Elliptic Curve Diffie-Hellman (ECDH) for generating secure public and session keys, while using certified public keys from certificate Authorities to ensure safe communication. Designed with a resource-constrained environment in mind, the system features a lightweight decentralized application (DApp) that enables secure interaction among registered voters, candidates, auditors, and validators [6].

Dong, Z. et al. conducted a comprehensive survey reviewing the evolution of voting systems, from traditional and electronic to blockchain-enabled methods. The study categorizes key elements necessary for implementing a blockchain-based e-voting system, including consensus protocol, frameworks, cryptographic standards, evaluation criteria, and development tools. It provides a thorough analysis of real-world implementation by government bodies, cooperation, and academic institutions, classifying them based on the problem they address, the blockchain infrastructure used, and their deployment status. Furthermore, it discusses persistent challenges such as privacy and security, evaluates current solutions, and outlines future research directions to build more trustworthy and widely accepted e-voting platforms [7].

Sugapriya M.et al. proposed a secure e-voting model built on the Ethereum network. The process begins with voter registration through a web interface, where users submit identity proof for verification. Once validated, voters are registered on the Ethereum network. A smart contract is then created to represent the election and encode rules, including the eligible voter list, candidates' details, voting duration, and victory condition. On election day, authenticated voters cast their votes by sending transactions to the smart contract. Once the voting period ends, the smart contract automatically counts the votes and announces the winner. The result remains publicly quarriable, ensuring transparency and immutability. However, the study notes challenges in safeguarding voter anonymity and preventing attacks on the Ethereum infrastructure [8].

Vairam T. et al. focused on a blockchain-based e-voting system using the Ethereum network, which relies on smart contracts and proof of work (PoW) consensus mechanisms. In this setup, Ether cryptocurrency powers the system, where new blocks are added by solving complex computational problems. The system ensures security and immutability, as any attempt to alter the voting data is reflected across the chain, making the system tamper-resistant and trustworthy [1].

III. PROPOSED METHODOLOGY

The proposed methodology for our blockchain-based E-Voting system is designed to ensure transparency, security, and trust throughout the entire voting process. The system architecture, as illustrated in Figure 3.1, begins with the admin, who serves as the central authority responsible for initiating and managing the election process.

DOI: 10.48175/IJARSCT-25618

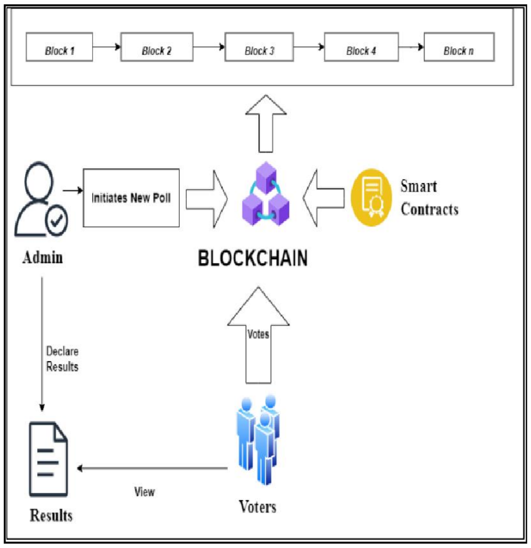


Fig 3.1: System Architecture

To start an election, the admin adds the list of eligible candidates and initiates a new poll. Once the poll is live, voters can securely cast their votes. Each vote is processed using a smart contract, which serves as a self-executing protocol that enforces the voting rule and ensures the integrity of the process without requiring manual intervention.

Every action in the system–whether it's the creation of a poll, the casting of a vote, or the declaration of a result—is recorded as a transaction on the blockchain. These transactions are grouped into blocks and added to the chain in a linear, chronological order. This ensures that once a vote is cast, it cannot be altered or tampered with, thereby providing a tamper-proof and verifiable record of all activities.

After the voting period ends, the system tallies the votes, and the admin declares the result. These results are also stored on the blockchain and made accessible to all voters, promoting transparency and trust.

By leveraging blockchain technology, this system eliminates the risks of vote manipulation and provides a decentralized, immutable, and auditable platform for digital election.

IV. PROPOSED WORK

Implementation of blockchain-based project. During the implementation, we encountered several challenges and the most important one faced was the implementation of Ether cryptocurrency. To overcome this we included a simulated currency system in the project, which allowed for seamless functionality without depending on actual cryptocurrency.

The project has been successfully implemented through the following steps:

A. Blockchain Deployment:

The voting application was hosted on Ethereum Virtual Machine (EVM). Smart contracts were written and executed to manage all the core functions, such as election creation, voter registration, casting of votes and tallying of results.

B. Election Instance Creation:

After deployment, we were able to successfully create election instances. This involved: Specifying election parameters like the name of the election, start time and end time of the election, and the list of candidates.

The finished system illustrates a working, secure and transparent blockchain based e-voting system.

DOI: 10.48175/IJARSCT-25618

C. Voter Registration:

Voters were able to link up to the blockchain in order to register. Providing personal information like blockchain account address, name and telephone number. Interacting with a registration smart contract that stored their data securely in a decentralized form.

D. Backend Processing:

After finalizing the voting and registration timeframes. Backend processes were invoked to: Finish the voting period according to the schedule specified in the smart contract. Automatically count the votes cast on the blockchain. Present the results of the election on a special results page, declaring the winner and showing a thorough overview of the voting statistics.

E. Security and Transparency:

Throughout the project, strong security measures were taken. Cryptographic techniques provided data confidentiality and integrity, while the decentralized nature of blockchain ensured complete transparency permitting all involved stakeholders to audit and verify the election process themselves.

F. Smart Contracts:

All core functionality registration, voting, and result counting was managed by smart contracts written in Solidity. The contracts successfully automated and enforced the election rules without the presence of intermediaries.

G. Admin Verification:

Admins use a special panel to inspect and authenticate voter registrations. Matching submitted blockchain account addresses and personal details with the admins official records. After verification, users were authenticated and allowed to vote in the election

H. Voting Process:

Verified voters used the voting interface to vote. The backend provided a smooth interaction with voting smart contracts, safely recording every vote on the blockchain. One vote per use enforcement, maintaining the sanctity of the election

I. Election Closure and Result Tallying:

At the end of the election duration, the admin officially ended the election through the admin panel. The last results were automatically calculated and displayed indicating the successful execution of the blockchain based e voting system.

V. IMPLEMENATATION AND EXPERIMENTAL SETUP

A. Frameworks:

- Blockchain Network: Ethereum (ETH)
- Local Blockchain: Ganache
- Testnet: GETH
- Smart Contracts: Truffle
- Backend: Node.js
- Frontend: React
- Web3js

B. Online Wallet:

- Browser Extension: MetaMask

DOI: 10.48175/IJARSCT-25618

C. Text Editor / IDE:

- VS Code
- Solidity

D. Smart Contracts Deployment Configuration

- Environment: Localhost
- Tools: Ganache
- Testnet: GETH

E. Hardware Requirements:

- Processor: Minimum Intel i3 or equivalent
- RAM: Minimum 4 GB
- Storage: Minimum 20 GB of free space
- Operating System: Minimum Windows 10, macOS 10.15+, or a Linux Distribution (Ubuntu 18.04+)
- Network: Stable Internet Connection for Smart Contracts Deployment and Blockchain Transaction

VI. SECURITY ANALYSIS AND THREAT MODEL

*A.Common Smart Contract Threats***:**

- Reentrancy Attack: A Callback function recursively calls the contract before the previous state updates.
- Front Running: Miners manipulate the orders of transactions for gain.
- Denial of service (DoS): An attacker prevents others from interacting with the contract.
- Gas Limit and Loops: Functions with unbounded loops may exceed the gas limit
- Timestamp Dependency: Logic that depends on the block timestamp, miners can manipulate this slightly

B. Threat Model: STRIDE Framework:

- Spoofing: A Hacker declares himself as an owner or Voter
- Tampering: Votes are Hacked and altered via Public Functions
- Information Disclosure: Voter Choices visible before deadline
- Repudiation: Voter Denies to cast a vote.

C. Security Measures Implemented:

- Access Control: Modifier used for administrative functions.
- Prevention from Double Voting: Boolean Flag (hasVoted) tracked for each voter
- Input Validation: require () Conditions for all statements
- No Loops: To prevent DoS, Voting Logic avoids dynamic iteration
- Reentrancy Protection: No External Calls before state updates

D. Cryptographic Assumptions:

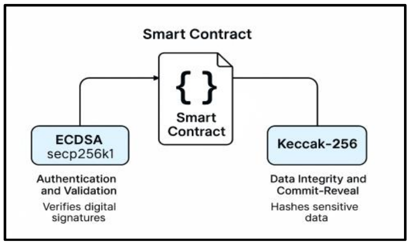

Smart Contract
{ }
Smart Contract
ECDSA
secp256k1
Authentication and Validation
Verifies digital signatures
Keccak-256
Data Integrity and Commit-Reveal
Hashes sensitive data

Fig 6.1: Cryptographic Assumptions

DOI: 10.48175/IJARSCT-25618

ECDSA (secp256k1): Elliptic Curve Digital Signature Algorithm

When a Voter or admin interacts with a smart contract, the Ethereum Blockchain verifies the digital signature of the transaction using ECDSA.

The msg.sender keyword in solidity confirms the identity of the caller, ensuring only the authorized users can perform the sensitive actions like Registering a Vote, Casting a Vote, etc.

Keccak-256: Ethereum's Hash Function

Voter's Choice is hidden by submitting a hash in real-time voting commitments using Keccak-256.

Hashing personal data like Email ID or Unique ID ensures privacy before storing it on a chain.

Ethereum Addresses are derived from the public key using Keccak-256 Algorithm.

VII. ETHICAL AND LEGAL CONSIDERATIONS

A. User Privacy and Data Protection

Ethical Concern: Storing Personal or Sensitive Data such as Voting Preferences, identity on a public ledger raises privacy concerns.

Legal Compliances: Must Comply with Data Protection Laws like

IT Act (India): Personal Data Protection under Section 43A.

CCPA (California): Data Access and Deletion Rights

B. Regulatory and Jurisdictional Challenges

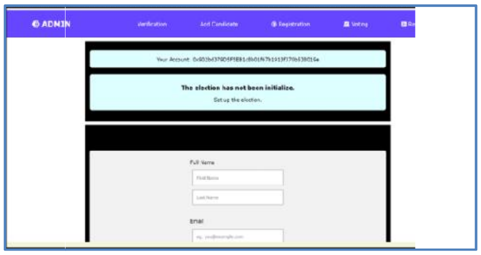
Ethical Concern: Blockchain Operates Globally but legal systems are jurisdiction-specific. In Some Countries, Blockchain tokens, smart contracts are not recognized legally.

Legal Compliance: Since this system is under educational experimental stage, local laws are adapted accordingly.

C. Ethical Use of Tokens or Incentives

Since Smart Contracts in this project use tokens, Fair Distribution and Accessibility is ensured. Also, Manipulation and Spacteculations are avoided.

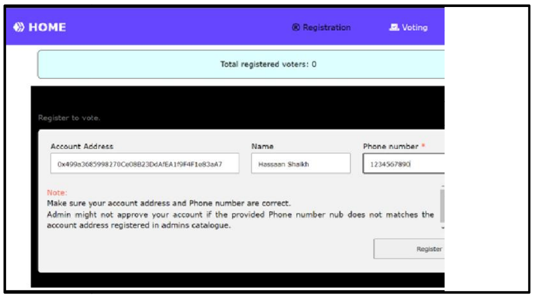
VIII. RESULTS



Your Account: [illegible]

The election has not been initialize.
Set up the election.

Fig 8.1: Admin Election Initialization



Total registered voters: 0

Register to vote.

Account Address: 0x499a3685998270Ce08B23DdAfEA1f9F4F1e83aA7

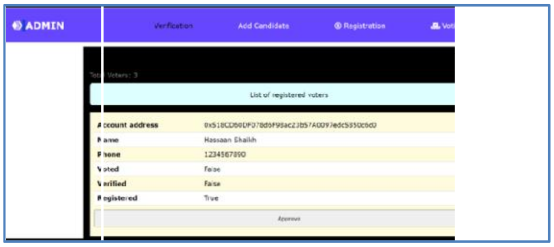
Name: Hassaan Shaikh

Phone number *: 1234567890

Note:
Make sure your account address and Phone number are correct.
Admin might not approve your account if the provided Phone number nub does not matches the account address registered in admins catalogue.

Fig 8.2: Voter Registration with Private Key

DOI: 10.48175/IJARSCT-25618

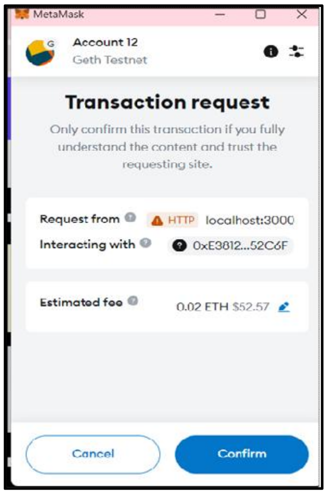


Total Voters: 3

List of registered voters

Account address	0x518CD60DF078d6F98ac23b57A0097edc5950c6d2
Name	Hassaan Shaikh
Phone	1234567890
Voted	False
Verified	False
Registered	True

Fig 8.3: Verification of Voter



Transaction request

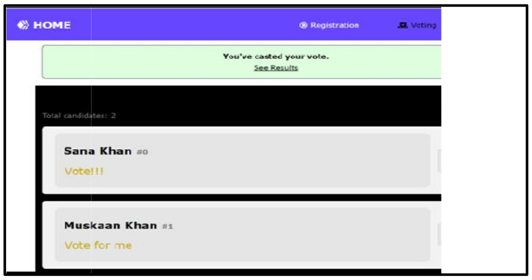
Only confirm this transaction if you fully understand the content and trust the requesting site.

Request from HTTP localhost:3000

Interacting with 0xE3812...52C6F

Estimated fee 0.02 ETH $52.57

Fig 8.4: Blockchain Transaction Confirmation



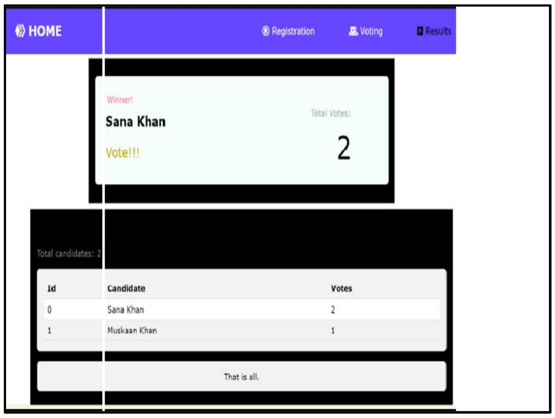
You've casted your vote.
See Results

Total candidates: 2

Sana Khan #0
Vote!!!

Muskaan Khan #1
Vote for me

Fig 8.5: Voting Page



Winner!
Sana Khan
Vote!!!
Total Votes:
2

Total candidates: 2

Id	Candidate	Votes
0	Sana Khan	2
1	Muskaan Khan	1

That is all.

Fig 8.6: Results

IX. FUTURE WORK

Introducing scalable consensus mechanisms: Implementing more efficient Consensus algorithms such as Proof-Of-Stake or Delegated Proof-Of-Stake can improve the Scalability and also reduce the Energy consumption.

Interoperability: A development system that can seamlessly integrate into existing Voting technologies and framework conditions to facilitate transition.

Improved voter authentication: Ensuring secure and complete voter authentication using Advanced biometric systems such as face recognition and fingerprint scanning.

Offline voting ability: Developing a mechanism that enables offline voting, while also keeping in mind that the votes are securely synchronized with the blockchain as soon as connectivity is restored.

X. CONCLUSION

In summary, the Blockchain-based electronic voting system project highlights the transformational potential of emerging technologies to ensure safe, transparent, and reliable elections. By using distributed, decentralized networks, smart contracts, and cryptographic techniques, the system ensures that votes are immutable, verifiable, and anonymous. As a result, the project is completed, providing a platform to promote trust in democratic processes and reduce the risk of manipulation and fraud.

We would like to thank all the participants who supported us during this trip. Our work shows how technology can strengthen society and democratic integrity. We want to continuously improve our system and expand its reach for wider acceptance in the future.

REFERENCES

[1] Sarathambekai, S., & Balaji, R.: “Blockchain-based voting system in the local network, 7th International Conference on Advanced Computing & Communication Systems” (ICACCS), 2021.

[2] Ibrahim, M., & Farooqui, O.: “ElectionBlock: An electronic voting system using blockchain and fingerprint authentication”, IEEE 18th International Conference on Software Architecture Companion (ICSA-C), 2021.

[3] Benabdallah, A., Audras, A., Coude, L., El Madhoun, N, & Badra.“Analysis of blockchain solutions for e-voting: A systematic review”, 2022.

[4] Chaudha, S, Shah, R., Gupta, A., Alabdulatif, A., Sharma, & Tanwar, S: “Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach”, IEEE, 2023.

[5] Pavan M, Navya D, Ajay Yadav R, Kausalya T, Kusuma H: “Blockchain-enabled e-voting system”, RTCS IT, International Journal of Engineering Research & Technology” (IJERT), 2023.

[6] Majumder, S, Ray, S., Sadhukhan, D., Dasgupta, M., Das, A.K., & Park, Y. (n.d). Exonum e-voting: A novel signature-based e-voting scheme using blockchain and zero-knowledge property,” 2023.

[7] Dong, Z. (n.d.): “E-voting meets Blockchain: A survey”, IEEE, 2023.

[8] Sugapriya, M. G., Hema, M. V., Subashini, M., & Swetha, M. D. (n.d).“E-voting system using Ethereum network”, NCAAIET, 2024.

[9] Shalini Shukla, A.N. Thasmiya, D.O. Shashank, H.R. Mamatha. "Online Voting Application Using Ethereum Blockchain", ICACCI, 2018.

[10] M. Iqbal and R. Matuleviˇcius, “Exploring Sybil and double-spending risks in blockchain systems,” IEEE, 2021.

[11] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, “E-voting systems using blockchain: An exploratory literature survey”, ICIRCA, 2020

DOI: 10.48175/IJARSCT-25618