



TrustChain: A Blockchain-Enabled Verifiable Digital Voting Solution for Election Integrity

Sonali Kothari^{1*}, Shweta Koparde², Shubham Joshi³, Namra Joshi⁴

¹ Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, India

² Department of Computer Engineering, Dr. DY Patil Institute of Technology, Pune 411018, India

³ Department of AI & DS, Vishwakarma Institute of Technology, Pune 411037, India

⁴ Department of Electrical Engineering, SVKM's Institute of Technology, Dhule 424001, India

Corresponding Author Email: sonali.kothari@sitpune.edu.in

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/isi.300308>

ABSTRACT

Received: 22 July 2024

Revised: 20 November 2024

Accepted: 7 December 2024

Available online: 31 March 2025

Keywords:

online voting, e-voting, blockchain, verifiable voting, Ethereum, Truffle, Metamask wallet

This research paper presents a comprehensive exploration of the development and implementation of a ground-breaking online voting platform, leveraging the transformative potential of blockchain technology. In response to the critical challenges of security vulnerabilities and transparency issues in conventional voting systems, the study highlights the strategic integration of blockchain's inherent decentralized and immutable properties. The project emphasizes creating an intuitive and user-friendly website interface, streamlining the voter registration process, enabling secure ballot submissions, and ensuring a transparent and accurate tallying of voting results. By harnessing the capabilities of smart contracts and advanced cryptographic techniques, the platform provides the confidentiality and integrity of the entire voting process, cultivating a heightened sense of trust and confidence among all participants. The proposed system delves into the intricate design elements. The meticulous implementation process behind developing an innovative online voting platform sheds light on the pivotal role of blockchain technology in safeguarding the integrity of the voting process, thereby instilling a sense of trust and credibility within the framework, and emphasizes the integration of smart contracts and cutting-edge cryptographic measures; the research highlights the platform's robust defense against potential security breaches and data manipulations, ensuring the sanctity of the voting data throughout the entire electoral journey.

1. INTRODUCTION

A distributed digital ledger called blockchain records transactions between multiple computers. This is the foundation of the technology that drives cryptocurrencies such as Bitcoin [1]. Among the different blockchains are public, private, hybrid, and consortium. Every variety has unique characteristics and fulfills a range of purposes. Blockchain is a data storage technique that makes system modification, hacking, and cheating difficult or impossible. As previously mentioned, a blockchain is a computer network that keeps a distributed, duplicate digital record of every transaction [1, 2].

The first person (or it may have been a group) to come up with the concept of a blockchain was Satoshi Nakamoto, who brought Bitcoin to life in January 2009. Bitcoin's blockchain was intended to record transactions in an entirely transparent, decentralized form that could not be altered. The trust mechanism of security allowed everyone to believe one another and prevented fraud. Blockchain creates a chain of blocks, each with a cryptographic hash of the previous block, a timestamp, and transaction data. The chain is maintained by one computer and verified by its peer over a network. It has no way to change the records of what it stores. Blockchain offers a secure, dispersed way to store or transmit information. It's

perfect for apps such as digital cash and clever contracts. The prospect of blockchain-based electronic voting systems transforming the political process by solving security, transparency, and verifiability issues has attracted much attention. Much work has been done in this area, producing insightful analysis and practical ideas for addressing the many problems connected with electronic voting and sorting out a strategy to solve them. To lay the foundation for dependable e-voting systems, the importance of security and verifiability in blockchain-based e-voting was stressed [1]. They proposed improving the voting process's security and trustworthiness. A similar critical look was taken at a blockchain-based electronic voting system established in Moscow [2]. It is pointed out potential problems and made suggestions for improvement. Through a test project, it was demonstrated that blockchain technology could make electronic voting safe and immune from manipulation [3].

2. LITERATURE REVIEW

An in-depth study on the current state of blockchain-based electronic voting systems was conducted [4]. The research examined existing implementations and identified key

challenges in the field, emphasizing the need for continuous improvements. Meanwhile, another study [5] explained how a blockchain-based electronic voting system was designed and demonstrated in actual practice, focusing on architectural considerations.

The development of a blockchain-based web portal to enhance security and interactivity was discussed [6]. By leveraging blockchain technology, the proposed system ensures secure storage and sharing of medical records, thereby improving patient data confidentiality and accessibility. Meanwhile, a decentralized e-voting system utilizing smart contracts and a private blockchain was proposed to enhance the security, transparency, and efficiency of elections in Iraq [7]. To ensure voter eligibility and data integrity, the system incorporates elliptic curve cryptography (ECC) and biometric authentication methods, such as QR codes, face recognition, and fingerprint scanning. The proposed solution addresses challenges associated with traditional voting systems, including fraud, accessibility, and timely results announcement.

The below part highlights the development of blockchain and blockchain-based voting systems worldwide.

- **Exploration of Blockchain's Potential Beyond Cryptocurrencies [8]:** The paper surveys blockchain-based e-voting systems, analyzing their security, transparency, and efficiency. It discusses various blockchain architectures, challenges, and potential improvements for secure digital voting.
- **Early Blockchain Voting Proposals [8]:** The first theoretical proposals for blockchain-based voting systems emerged. These early models envisaged using a public blockchain (e.g., Bitcoin) for secure voting, with transparency, immutability, and the ability to verify votes' anonymity still in place.
- **Development of Initial Blockchain Voting Prototypes [9]:** Some research teams and technology companies started building prototypes to experiment with whether blockchain could work for voting. Pilot projects and case studies, including small-scale elections, were held to show that using blockchain for voting was a potential boon. One benefit of this was preventing vote tampering. Another critical point is that blockchain makes it possible to see precisely what has been done.
- **Blockchain Voting Trials at the University of Hong Kong and the Swiss Post:** The University of Hong Kong initiated a trial where students could vote using blockchain technology. This was one of the first real-world trials, although it was limited in scope [10]. Swiss Post also initiated a blockchain-based pilot voting system to determine whether distributed ledger technology could be used for secure elections [11].
- **Estonia's bid to replicate blockchain technology for e-voting demonstration [12]:** Estonia has long been a champion of digital governance. It has ventured into using blockchain technology to register citizens' residency or cast votes through this form. Estonian e-voting implemented blockchain technology in 1995; it was intended to be secure for voters and prevent fraud. Estonia continued exploiting blockchain to provide more government services digitally, including Internet voting. Blockchain has been increasingly incorporated into the existing system to protect further and strengthen its (e-)voting infrastructure.

With the development of blockchain technology and the popularization of Bitcoin and other virtual currencies, many central government bodies and private businesses have sought to put such means into use for democratic processes. A significant milestone in 2017 was using smart contracts on the Ethereum platform to build voting systems. Implementing this technique made more flexible solutions for verifying, logging, and counting votes possible.

- **Blockchain Voting in U.S. Elections by Voatz [13]:** The mobile voting platform Voatz applied its blockchain-based voting system to trial elections, including West Virginia's midterm elections in the United States. Through Voatz, all military personnel on active service overseas could cast their votes as usual from their smartphones. In this particular instance of applying blockchain technology to election systems, it guaranteed the security and immutability that only found escorts can provide. Voatz's implementation ran on Hyperledger Fabric, a permission-free blockchain, to provide advanced privacy and scalability. The 2018 Voatz test was part of the trend to try out blockchain in real-life election settings, with the program coming under attack for potential vulnerabilities.
- **COVID-19 and the Rise of Digital Voting [4]:** The virus forced municipalities to set up remote voting systems because the traditional in-person voting system has limitations. Blockchain voting systems began, in turn, to appear more attractive, with the capacity to secure elections and deter fraud. The 2020 US presidential election saw blockchain-based e-voting rise as a potential way out from mail-in ballot disorder and election security worries.

In line with the maturing of blockchain voting, hybrid systems (public and private chains combined) were beginning to take shape to strike a balance between privacy, scalability, and transparency. However, this wove in the demands of the regulatory environment to produce systems with far more flexibility and robustness [14]. With the rapid progress of blockchain projects, identity verification has become an important issue. By using blockchain technology to prove a voter's identity securely, election fraud can be further resisted. Talks about setting global standards for blockchain voting systems began. Legal bodies and international organizations are looking at the legal and technical aspects of Dapp voting to build stable and publicly trusted systems—especially in government elections. They try to balance regularity with freedom to trade [15, 16].

- **Principal Issues and Future Directions [17]:**
 - (1) **Security:** Despite advances in security, one primary concern is the possibility of cyber-attacks, especially voter identity protection, and preventing blockchain nodes from being tampered with.
 - (2) **Scalability:** The sheer scale of transactions and fees with national elections presents a significant problem for blockchain systems, especially in public ones.
 - (3) **Regulation and Legal Frameworks:** Global standards are needed for blockchain-based voting systems, as well as a new legal framework to ensure that these systems are in keeping with democratic principles and electoral integrity.
 - (4) **Voter Confidentiality:** Carving out space for confidential voting, a fundamental problem nowadays is ensuring privacy while preserving transparency. One possible answer is to develop new cryptographic

techniques, such as zero-knowledge proofs. Table 1 reviews various research papers and studies in the field

about different voting systems and methodologies proposed using multiple blockchains.

Table 1. A systematic comparison of blockchain-based voting systems

Refs	Methodology	Findings	Drawbacks
Kiayias and Yung [18]	Proposed a cryptographic framework for secure electronic voting using blockchain principles.	Demonstrated the feasibility of using blockchain for secure voting.	Limited scalability for large-scale elections.
Hao et al. [19]	Developed a secure multi-party computation protocol for anonymous voting.	Ensured voter privacy while maintaining verifiability.	Computational complexity may hinder real-time applications.
McCorry et al. [20]	Implemented a smart contract for boardroom voting on the Ethereum blockchain.	Achieved self-enforcing e-voting without trusted authorities.	Potential vulnerabilities in smart contract code.
Hao et al. [21]	Trialed a Direct Recording Electronic (DRE) system with enhanced privacy features; conducted a trial of the DRE-ip system in a UK polling station	Provided end-to-end verifiability without tallying authorities, received positive voter feedback, and demonstrated practicality.	User acceptance and trust in technology were concerns; limited to small-scale trials, scalability remains a question.

3. METHODOLOGY

This section describes the techniques for creating and deploying the proposed blockchain-powered online voting platform, covering design, user interface development, security protocols, and blockchain platform selection.

Designing wireframes and developing user interfaces - Figma, a design tool renowned for its capacity to build precise wireframes, will be used to create wireframes, which serve as blueprints for constructing websites. The proposed project will create the user flow, arrange the parts in the right places, and visualize the website's structure thanks to Figma. The wireframes will be created according to user expectations and usability standards to ensure a user-friendly and intuitive interface.

Using the Telos platform over Ethereum gives it better security, decentralization, speed, and scalability. A Proof of Stake (PoS) mechanism is used on Telos, unlike Ethereum's Proof of Work (PoW). It is not only more power efficient but also capable of higher throughput. Telos will keep the proposed voting system decentralized and easy to use but is designed to enhance its performance, scalability, and security in general. Aesthetic Interface and Ease of Use Goals for the voting system include increased security, ease of use, and an interface visual presentation. The system is concerned with enhancing voter convenience and participation, especially among traditionally disadvantaged groups. People will be shown how to vote through an appealing and user-friendly interface that gives clear directions of a person's level of technological prowess. With biometric and multi-factor authentication techniques, genuine elections will use identity verification. The methods ensure the individuality and authenticity of every voter, and a well-thought-out user interface is crucial in guiding voters through the verification process. Security steps: It is critical that cryptographic security protocols protect the voting process adequately and thoroughly enough so that testing and simulations can be done. The technology is designed to produce a traceable and verifiable digital path for voters, assuring the electoral process. The system employed in actual elections by independent auditors ought to be extraordinarily reliable and resistant to manipulation.

While retaining low transaction fees, Telos is also faster than Ethereum. Although Ethereum can perform 14

transactions per second (TPS), it has been known to crash under workloads of tens of thousands. Telos, on the other hand, supports up to 10,000 transactions every second. The EVM compatibility of Telos makes Ethereum smart contracts easy to deploy. Using a unique Proof of Capacity (PoC) consensus method to ensure that every transaction is on the block, Telos also rewards users with the storage of data, which means improved security and decentralization. On the other hand, Telos users are equivalent to the shareholders of a company. Without central headquarters, Telos is controlled and managed solely by its community members through a decentralized voting system, allowing only supporters to influence operational direction and design! These are excellent reasons developers and clients should switch from Ethereum to Telos: Transaction speed — Cost reduction — Because it is just like Ethereum's smart contracts. Table 2 helps in understanding Telos's features compared to similar and existing blockchain platforms.

These enhancements could make a blockchain-based electronic voting system more transparent, secure, and user-friendly while also heightening confidence in the honesty of the election results.

System Architecture Plan - The system architecture plan contains the entire system's architecture and how voting will be implemented. As can be seen from the diagram, this voting system has many vital inputs, processes, and outputs. The input includes election parameters, candidate details, and voter registration information, which are maintained securely in a database built on blockchain technology. Candidates register by submitting their details and election parameters, whereas voters register once they have given their personal information. Using a blockchain-based voting tool, votes are cast, and results are encrypted and stored in one database. After the election, the ballots are counted, results are announced, and the blockchain database is updated. The system's data transmission is orderly. All of the voter registration data, candidate details, and election settings are incorporated into the blockchain database to ensure the secrecy and transparency of the election. Once a vote has been cast, it is securely stored in the database, informing both the organizers of the election and members of the public of its outcome. By verifying voter registrations and providing a simple, reliable way to determine election results, this method builds the public's trust in democratic processes.

Table 2. Comparison of telos with other blockchain platforms

Feature	Telos	Ethereum	Solana	Binance Smart Chain	Cardano
Consensus Mechanism	Delegated Proof of Stake (DPoS)	Proof of Stake (PoS)	Proof of History (PoH) + PoS	Proof of Staked Authority (PoSA)	Ouroboros (PoS)
Transaction Speed	~0.5 seconds	~12-14 seconds	~400ms	~3 seconds	~20 seconds
Scalability	High	Moderate	Very High	High	Moderate
Transaction Fees	Minimal	High	Minimal	Low	Minimal
Smart Contract Support	Yes, Ethereum-compatible	Yes	Yes	Yes	Yes
Unique Features	Energy-efficient supports ESG initiatives	Largest developer ecosystem	Ultra-fast transactions, high throughput	Binance ecosystem integration	Strong focus on academic research
Governance	On-chain governance	Limited on-chain governance	Centralized at the validator level	Centralized validators	Community-focused governance
Environmental Impact	Low	Moderate	Low	Moderate	Low

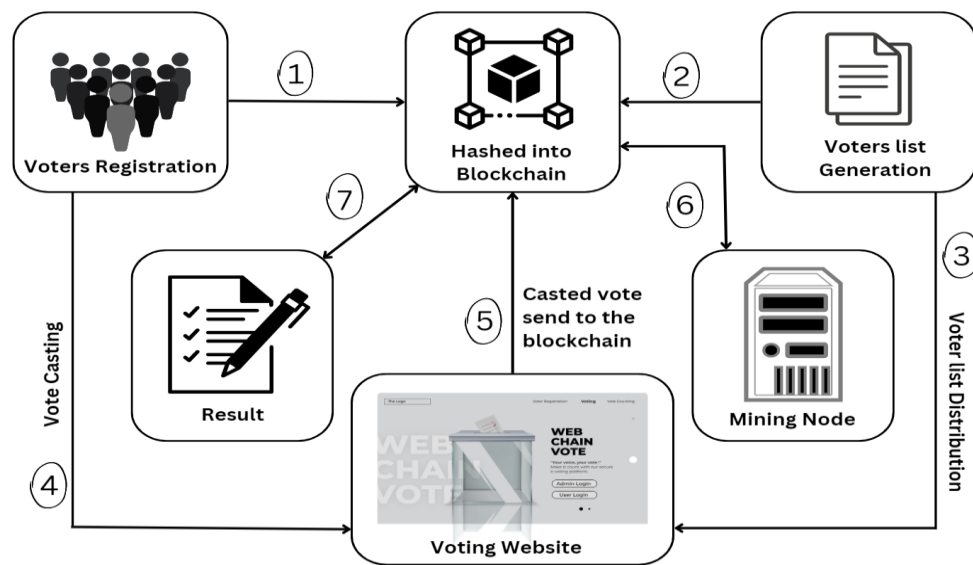
**Figure 1.** Flow diagram of the proposed methodology

Figure 1 highlights the block diagram of the proposed research work.

To ensure that online ballots are secure and free of tampering, the new e-vote technology and blockchain technology are implemented.

Key Components User interface:

1. Voter Login: Voters enter their credentials on the website's interface. Vote Casting Voters utilize an easy and user-friendly interface to cast their votes.
2. Anonymity: The system protects the voter's identity, while vote matters remain confidential.
3. Blockchain: Votes are Transactions: Every vote is carried out as a transaction and added to the blockchain. Transaction Validation Once a vote comes in, the blockchain network will validate it before recording this transaction. Data That Can't Change After a transaction is on the blockchain, it is immutable. This means it cannot be altered or eradicated, providing the vote's authenticity can be trusted.

MongoDB (Backend):

1. Storage: To ensure candidate information, voter data without any accurate discernible personal details (i.e., anonymous voting), and even election statistics remain

safe, the voting details are all kept in MongoDB's database.

2. Auditability: The election details may be easily called back for audit using the database without endangering data security or privacy.
3. Scalability: MongoDB can contain large quantities of data to handle significant elections and thus has been employed here to keep the system scalable. Details of candidacy and votes on blockchain:
4. Non-disclosure of Votes: To keep them confidential, each vote is encrypted before it's put onto the blockchain.
5. Election Data on Blockchain: Information about candidates and votes, including tallies where appropriate, is kept on the blockchain. And that makes democracy transparent anew—little as Sunshine.

Methodology:

1. Voter Register and Verification: Voters are registered and verified securely (biometric passwords, 2FA, etc.).
2. Cast Votes onto Blockchain: Once verified, the voter chooses their candidate to vote, and then a transaction on the blockchain is recorded for this vote. Finally, the transaction to register that vote on the blockchain is verified and added to the blockchain.

3. Data Security: Sensitive information such as votes and one's secure identification are encrypted, ensuring that even the user sending it is all private information.
4. Audit and Transparency: Because of the nature of the blockchain, oversight of the entire operation is easy, even in elections. The process can be calculated by external third parties or systematically analyzed to see whether any part has been distorted.
5. Security: Blockchain enables every vote to be authenticated; once inserted into the blockchain, it can never be changed again. The privacy of voters is further protected by encrypting data in transit.
6. Transparency and Trust: Blockchain makes the operations of the voting public so all can verify that a count was taken down correctly, even without ever visiting any poll site themselves.
7. Scalability: The system is built to handle many electors and contests, and if necessary, it can grow.
8. Auditability: A MongoDB backend and a blockchain provide excellent means for safely auditing elections so

that results may be objectively judged even remotely.

This system combines the immutability and transparency of the blockchain with a front end. One can use back-end scalability; together, it offers secure and efficient e-voting services.

```
pragma solidity ^0.5.16;
contract Migrations {
    address public owner;
    uint public last_completed_migration;

    modifier restricted() {
        if (msg.sender == owner) _;
    }

    constructor() public {
        owner = msg.sender;
    }

    function setCompleted(uint completed) public restricted {
        last_completed_migration = completed;
    }
}
```

Figure 2. Migrations smart contract

```
pragma solidity ^0.5.16;
contract Election {
    struct Candidate {
        uint id;
        string name;
        uint voteCount;
        string details;
        string election_id;
    }
    mapping(uint => Candidate) public candidates;
    mapping(address => bool) public voters;
    uint public candidatesCount;
    string public candidate;
    constructor() public {}
    event votedEvent(
        uint indexed _candidateId
    );
    function addCandidate(string memory _name, string memory _details, string memory _election_id) public {
        candidatesCount++;
        candidates[candidatesCount] = Candidate(candidatesCount, _name, 0, _details, _election_id);
    }
    function vote(uint _candidateId) public {
        require(!voters[msg.sender]);
        require(_candidateId > 0 && _candidateId <= candidatesCount);
        voters[msg.sender] = true;
        candidates[_candidateId].voteCount++;
        emit votedEvent(_candidateId);
    }
}
```

Figure 3. Election smart contract

The smart contract (Figure 2) provided, "Migrations," is a utility contract used in the deployment process of Ethereum-based smart contracts, often with tools like Truffle running on them while deployed by a contract transaction. The contract keeps track of the number and location in each deployment of the contract migrations step, so any deployment step happens only once. Other Properties The contract gives the address responsible for creating and owning the contract. This role allows certain functions throughout the contract via a protective modifier. When the `last_completed_migration` variable is updated by this function and qualified by a protected modifier, this reflects that a particular migration has been completed. This avoids duplicate or erroneous migrations when the transactions involved in contract upgrades are posted and blow their precompile limit. In practice, this works as follows: When called, `setLastCompletedMigration` stores 'step_nr' in century at `spotstep_for` (centuries); Elsewhere, since `step_nr` has been completed, "step_nr" in new century is preserved, which provides information about how many generations were sent before it indexed below either hint or

correspondingly for wast lists. This avoids re-deploying or repeating the migration steps altogether by performing with external pure calls during the stage of business, prevents contract updates, and re-deployments reliance on placed code is more.

The election smart contract (Figure 3) writes a basic election system on the Ethereum blockchain. The agreement describes a Candidate structure, including fields such as ID, name, vote count, details, and election_id. It permits anyone wishing to stand for election to register as a candidate along with additional metadata. Candidates are stored in map candidates with IDs as keys; the number of candidates is indicated by the candidates count. Also included in the contract is a mapping voter, which makes sure each voter can only vote once so long as it has been set to true. The `addCandidate` function can add a candidate for the election, while the `vote` function allows users to vote for candidates through their numbers ID for the candidates by their ID. It ensures that only legitimate candidates will be voted by voters and prohibits double voting. When a vote is successful, after it

has been cast and is final, an event called votedEvent is activated. According to it, off-chain applications can then track the election's progress in near-real time! Integrity, transparency, and immutability are the cornerstones of this simple blockchain-based election on the chain.

4. RESULTS AND DISCUSSION

1. Implementation of Backend (MongoDB) - The backend handles the server-side logic of the proposed application. It manages user authentication, processes votes, and stores data. Node.js is a runtime environment that allows you to run JavaScript on the server. It's well-suited for building scalable, event-driven applications. MongoDB is a NoSQL database that can store user information, election data, and voting records. Together, Node.js and MongoDB provide the necessary infrastructure for the backend of the proposed voting system.
2. Implementation of Frontend (React.js) – The front end is the user interface of the proposed voting system, where users interact with the application to cast their votes and view election results. React.js is a popular JavaScript library for building user interfaces. It enables the creation of dynamic, responsive, and user-friendly web applications. In the context of a voting system, React can display election choices, allow users to cast votes, and show real-time results.
3. Ganache for Testing and Truffle for Compilation (Figure 4) - Ganache is a local blockchain emulator for testing and development. It helps to test proposed smart contracts and systems in a controlled environment. Testing is crucial in blockchain development to ensure that proposed smart contracts and the overall system work as expected. Ganache provides a simulated blockchain environment where it is possible to test various scenarios, ensuring the reliability and correctness of the proposed voting system.

4. Implementation of Metamask for transactions – Metamask is a cryptocurrency wallet and gateway to blockchain applications. It allows users to sign transactions securely, making it a vital component for ensuring the integrity of votes. The proposed voting system is used to sign and record votes on the blockchain, guaranteeing the authenticity and security of the voting process.
5. Truffle is a development framework for Ethereum and other blockchain platforms. While the proposed project migrated to Telos, Truffle may still be used for innovative contract development, compilation, and deployment. Truffle streamlines the development process by providing tools for compiling, testing, and deploying smart contracts. Even when deploying on Telos, it can be used for initial intelligent contract development and testing.

Figure 5 shows snapshots of the frontend design. The admin will have the function to add and manage an election on the website, add candidates, set voting date, time, and duration, and view vote count or display the results. In contrast, the users have the option to enroll in the available election and cast a vote on the website.

The performance analysis of the proposed system is discussed in Table 3, Table 4, and Table 5.

Table 3 overviews the system's hardware and software specifications, including processor type, memory capacity, storage, operating system, and any dependencies required for optimal performance. Table 4 outlines the critical metrics used to evaluate system performance, such as transaction speed, latency, throughput, security measures, and resource utilization, to assess the efficiency of the blockchain-based voting system. Table 5 lists the tools, frameworks, and environments used for testing the blockchain voting system, including simulation software, benchmarking tools, network configurations, and testing methodologies to ensure reliability and security.

```
2_initial_migration.js
=====

Replacing 'Election'
-----
> transaction hash: 0x4fa7942bb16f2bc71e429c5a134d5e78108b47f2e77883decbf4c5ab57a19dc5
> Blocks: 0        Seconds: 0
> contract address: 0x896Aa4F2bEed0377dB3eDCB09619d08f21fa38A0
> block number:    3
> block timestamp: 1697529750
> account:         0xe3a77945cE544aE817204CbE6968a7a93639af6d
> balance:         99.997277520605669056
> gas used:        634275 (0x9ada3)
> gas price:       3.175945008 gwei
> value sent:      0 ETH
> total cost:      0.0020144225199492 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:      0.0020144225199492 ETH

Summary
=====
> Total deployments: 2
> Final cost:      0.0025728601449492 ETH
```

Figure 4. Compilation using Truffle


The Logo

Polls

Add Poll

Vote Counting

Add various details of the election below.



ADD POLL

Poll Title

Description

Start date

21-08-2023

End date

23-08-2023

Start time

End time

Add Images

Create Poll

Figure 5. Admin login to create a poll

Table 3. System configuration summary

Component	Configuration
Operating System	Windows
CPU	Quad-core (Intel i7)
RAM	16 GB
Storage	1 TB SSD
Network	1 Gbps Ethernet
Blockchain Setup	Ganache (Ethereum emulation)
Metamask	Latest version
MongoDB Version	4.4.x or higher
Frontend	React.js, Node.js 14.x LTS
Database	MongoDB
Testing Tools	Truffle, Ganache

Table 4. Key performance indicators

Key Performance Indicator	Definition	Voter Scale	Test Results	Analysis
System Response Time	The system takes time to respond to user actions such as casting a vote or retrieving results.	10 users	~0.1 seconds	System response time is minimal and fast due to the lightweight nature of the application at low user scales, where MongoDB and Node.js handle the requests efficiently.
		50 users	~0.2 seconds	Response time increases slightly as the user load increases but remains within acceptable limits, showcasing the scalability of Node.js backend and React frontend.
		100 Users	~0.5 seconds	The response time remains manageable even under moderate user load, reflecting the effectiveness of the backend (Node.js) and database (MongoDB) in handling user interactions.
Transaction Processing Capability (TPS)	Number of transactions (votes) processed per second.	10 users	150 TPS	The system processes votes quickly and efficiently under low load, with MongoDB managing vote data and the backend supporting a high volume of transactions per second.
		50 users	140 TPS	There is a slight decrease in transaction processing as the number of users increases, but it can still handle medium-scale elections. Ganache's testing environment helps simulate the actual blockchain performance.
		100 Users	130 TPS	There is a decrease in TPS with a more extensive user base, but the system continues to perform well within acceptable limits for online voting applications, even under moderate load.
Storage Overhead	Data storage requirements for user, election, and transaction data in MongoDB and blockchain.	10 users	MongoDB: ~2 MB, Blockchain: ~10 KB	There is low storage overhead for MongoDB and blockchain, as the data volume is small, and MongoDB's NoSQL database structure efficiently stores user and voting data.
		50 users	MongoDB: ~10 MB, Blockchain:	The storage overhead increases with more users, but the MongoDB NoSQL structure scales efficiently, handling larger data volumes. Blockchain storage remains minimal due to the

100 Users	~50 KB	lightweight nature of the vote records.
	MongoDB: ~20 MB, Blockchain: ~100 KB	The system can handle larger data volumes as the user base grows. MongoDB continues to scale well, and the blockchain overhead remains modest. Storage overhead for both components remains manageable within real-world constraints.

Table 5. Testing tools and environment summary

Component	Tool/Framework Used	Purpose
Backend	Node.js, MongoDB	Handled server-side logic, data storage, and response time testing under varied loads.
Frontend	React.js	Ensured responsive user interface under simulated high-traffic scenarios.
Blockchain Testing	Ganache	Simulated blockchain environment for transaction processing and performance measurement.
Transaction Signing	Metamask	Verified secure and seamless vote signing and recording under real-world scenarios.

5. CONCLUSIONS

With its use of the Ethereum blockchain network in both the implementation process and hardware features, this vote has shown great potential to alleviate deficiencies experienced with existing voting methods. Integrating intelligent contracts (distribution management systems) and distributed ledger technology has guaranteed security, transparency, and fairness in the voting process. With an Ethereum blockchain voting system, this gives everyone confidence that their vote counts. Ethereum blockchain has to assist voting religion and voting privacy better safeguards in place; exerted complex process control intensive engineering, original signed transactions control cannot be lost except by error; Everything that can't ever happen told backward: every coin of credit has been lost of this bill banks know only those who reveal themselves for work have your word behind them before anything else becomes practical enough to speak its idea finally those being created means these people get to have their say in terms of a salary and after that get to enjoy their day working side-by-side on politics Television announcers from so many different countries confirmed that 6 million ether tokens.

Future Scope: The potential future scope of a blockchain-based voting system project is encouraging and could include several improvements and developments, such as ongoing security measures improvement, increased accessibility through user-friendly interfaces and mobile apps, advanced identity verification methods implemented, scalability for larger voter volumes ensured, enhanced privacy measures enhanced with advanced cryptographic techniques, expanded use of blockchain for election-related activities, exploration of blockchain interoperability, global collaboration to promote international adoption, investment in research and development, robust legislative framework establishment, independent auditing mechanisms implemented, and public awareness campaigns This dynamic future scope seeks to introduce a more safe, transparent, and effective voting system, thereby changing the electoral environment.

REFERENCES

- [1] Badertscher, C., Gaži, P., Kiayias, A., Russell, A., Zikas, V. (2018). Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 913-930. <https://doi.org/10.1145/3243734.32438>
- [2] Vakarjuk, J., Snetkov, N., Willemson, J. (2022). Russian federal remote E-voting scheme of 2021—protocol description and analysis. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference, pp. 29-35. <https://doi.org/10.1145/3528580.352858>
- [3] Pawar, D., Sarode, P., Santpure, S., Thore, P., Nimbalkar, P. (2019). Secure voting system using blockchain. International Journal of Engineering Research & Technology (IJERT), 8(11): 817-819. <https://doi.org/10.17577/IJERTV8IS110414>
- [4] Jafar, U., Aziz, M.J.A., Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors, 21(17): 5874. <https://doi.org/10.3390/s21175874>
- [5] Chatterjee, U., Ray, S., Adhikari, S., Khan, M.K., Dasgupta, M. (2023). Efficient and secure e-voting scheme using elliptic curve cryptography. Security and Privacy, 6(3): e283. <https://doi.org/10.1002/spy2.283>
- [6] Tidke, S.K., Khedkar, V., Banerjee, A., Mulik, A., Goyal, A., Chhabaria, Y. (2022). An interactive and secure blockchain web portal for online healthcare services. In 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand, pp. 454-459. <https://doi.org/10.1109/DASA54658.2022.9764973>
- [7] Jumaa, M.H., Shakir, A.C. (2022). Iraqi e-voting system based on smart contract using private blockchain technology. Informatica, 46(6). <https://doi.org/10.31449/inf.v46i6.4241>
- [8] Abuidris, Y., Kumar, R., Wenyong, W. (2019). 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, pp. 99-104. <https://doi.org/10.1145/3376044.3376060>
- [9] Chafiq, T., Azmi, R., Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. International Journal of Intelligent Networks, 5: 38-48. <https://doi.org/10.1016/j.ijin.2024.01.004>
- [10] Yu, B., Liu, J.K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., Au, M.H. (2018). Platform-independent secure blockchain-based voting system. In Information Security: 21st International Conference, ISC 2018, Guildford, UK, pp. 369-386. https://doi.org/10.1007/978-3-319-99136-8_20
- [11] Swiss Post (2023). Exclusive insight into Swiss Post's e-voting system. <https://digital-solutions.post.ch/en/e-voting>

- government/blog/exclusive-insight-into-swiss-post-s-e-voting-system.
- [12] Cong, L.T.Q., Thuy, N.D.P., Nhi, H.T.N., Anh, T.V. Blockchain-based electronic voting: Lessons from Estonia. *Vietnamese Journal of Legal Sciences*, 11(2). <https://doi.org/10.2478/vjls-2024-0009>
- [13] Specter, M.A., Koppel, J., Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in U.S. federal elections. In *Proceedings of the 29th USENIX Security Symposium*. <https://www.usenix.org/conference/usenixsecurity20/presentation/specter>.
- [14] Vivek, M., Anusuya, K. (2024). Secured and decentralized system for e-voting with hybrid cryptography and blockchain. *IETE Journal of Research* 70(11): 8278-8290.
- [15] Russo, A., Anta, A.F., Vasco, M.I.G., Romano, S.P. (2021). Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. In *2021 IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, pp. 417-424. <https://doi.org/10.1109/Blockchain53845.2021.00065>
- [16] Kim, H., Kim, K.E., Park, S., Sohn, J. (2021). E-voting system using homomorphic encryption and blockchain technology to encrypt voter data. *arXiv preprint arXiv:2111.05096*. <https://doi.org/10.48550/arXiv.2111.05096>
- [17] Taş, R.; Tanrıöver, Ö.Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry*, 12(8): 1328. <https://doi.org/10.3390/sym12081328>.
- [18] Kiayias, A., Yung, M. (2003). Robust verifiable, non-interactive zero sharing: A plug-in utility for enhanced voters' privacy. In *Advances in Information Security*, Springer, Boston, MA, pp. 139-152. https://doi.org/10.1007/978-1-4615-0239-5_9
- [19] Hao, F., Ryan, P.Y., Zieliński, P. (2010). Anonymous voting by two-round public discussion. *IET Information Security*, 4(2): 62-67. <https://doi.org/10.1049/iet-ifs.2008.0127>
- [20] McCorry, P., Shahandashti, S.F., Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. In *Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta*, pp. 357-375. https://doi.org/10.1007/978-3-319-70972-7_20
- [21] Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S. F., Mehrnezhad, M., Toreini, E., Metere, R., Liu, L.Y. (2020). End-to-end verifiable e-voting trial for polling station voting. *IEEE Security & Privacy*, 18(6): 6-13. <https://doi.org/10.1109/MSEC.2020.3002728>