JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE ONLINE VOTING SYSTEM USING BLOCKCHAIN

[1] Mr.K.Sadanandam, [2] Ms. Aamena Suzzanne, [3] Ms. Sree Harshitha, [4] Mr. Syed Riyan
[1]Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.
[2,3,4] B-Tech students, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.

***Abstract*—** In any democratic country, Voting is a fundamental right of any citizen that enables them to choose the leaders of tomorrow. It gives individuals in a community the facility to voice their opinion. It helps them realize the importance of citizenship. Online voting systems are software platforms used to securely conduct votes and elections. As a digital platform, they eliminate the need to cast your votes on paper or in person. They also protect the integrity of your vote by preventing voters from being able to vote multiple times. Electronic voting, or e-voting has fundamental benefits over paper based systems, such as increased efficiency and reduced errors. The electronic voting system tends to maximize user participation, by allowing them to vote from anywhere and from any device that has an internet connection. The blockchain is an emerging, decentralized, and distributed technology with strong cryptographic foundations that promises to improve different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns about e voting. Here, we propose a blockchain-based voting system that will limit voting fraud and make the voting process simple, secure, and efficient..

Keywords— *E-Voting, Electronic Voting, Blockchain Technology, Voting Fraud Prevention, Security, Efficiency, Transparency, Decentralization, Distributed Ledger, Cryptography, Voter Privacy, Trustworthiness, Authentication, Verification, Ballot Integrity*

I. INTRODUCTION

Voting stands as a cornerstone of democracy, embodying the collective will of the populace in selecting representatives and shaping governments. Over time, the concept of voting has evolved into a crucial tool for expressing choice and instilling trust in the democratic process. As democratic institutions gain credibility and acceptance worldwide, ensuring the integrity and transparency of the voting system becomes paramount. However, numerous instances in various countries have highlighted deficiencies in traditional voting methods, ranging from transparency issues to logistical challenges. To address these shortcomings and bolster confidence in the voting process, leveraging technology emerges as a promising solution.

In response to the imperfections of traditional voting systems, innovative approaches leveraging technology have emerged to modernize the voting process. Among these, blockchain technology offers a secure, efficient, and transparent platform for conducting elections. By harnessing the decentralized nature of blockchain, along with robust cryptographic techniques, voting systems can ensure the integrity of the electoral process

while safeguarding the anonymity and privacy of voters. Moreover, the convenience and accessibility

afforded by blockchain-based e-voting platforms have the potential to significantly increase voter turnout, particularly in regions with historically low participation rates.

India, with its vast population and diverse electorate, presents a compelling case for the adoption of blockchain-based voting solutions to address longstanding challenges in the electoral process. With millions of eligible voters yet to participate in elections due to logistical constraints and concerns over fairness, a technologically advanced voting system holds promise in overcoming these barriers. By leveraging web-based applications built on blockchain, coupled with robust security measures and user-friendly interfaces, India can enhance voter engagement, ensure the accuracy of election results, and uphold the principles of democracy.

II. LITERATURE SURVEY

[1] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson propose a novel approach to electronic voting. They introduce a decentralized e-voting system that prioritizes fairness, privacy, transparency, and flexibility, leveraging blockchain technology to address the limitations of traditional systems. By evaluating popular blockchain frameworks, they aim to construct a secure and cost-effective e-voting system, demonstrated through a detailed case study illustrating the potential of distributed ledger technologies to enhance the integrity of nationwide elections.

[2] FREYA SHEER HARDWICK, The author presents the first step of e-voting using a decentralized e-voting system with voter privacy rights, employing smart contracts and PKIs for verification and digital signatures that are extremely reliable and

effective. The protocol has been created to follow basic e-voting principles, allow for a certain amount of decentralization, and allow voters to modify or update their votes.

[3] King-Hang Wang, Subrata K. Mondal, Ki Chan, and Xiaoheng Xie, highlight electronic voting as a longstanding area of research spanning over 30 years, yet its widespread adoption remains a distant prospect due to significant security and trust challenges. Their study delves into the complexities of electronic voting systems, emphasizing the paramount importance of security measures to engender confidence among voters. By analyzing existing literature, they compile a comprehensive list of security specifications crucial for developing secure electronic voting systems. Additionally, they examine both theoretical and real-world e-voting systems, as well as usability studies, to glean insights into enhancing user-friendliness.

[4] D. A. Gritzalis, underscores the potential of electronic voting (e-voting) to enhance democracy in modern information societies. However, he emphasizes the necessity for e-voting systems to comply with legal and regulatory frameworks while meeting user requirements. Gritzalis outlines two key objectives: firstly, to delineate constitutional requirements essential for the development of e-voting systems for general elections, ensuring adherence to court-acceptable design guidelines. Secondly, employing the Rational Unified Process, Gritzalis aims to ascertain the requisite level of security for e-voting systems.

[5] Shekhar Mishra examines the utilization of electronic voting systems in Indian general and state elections, identifying security concerns as a major drawback. Specifically, they highlight the vulnerability to voter impersonation, where unauthorized individuals cast ballots using others' identities. Their proposed solution utilizes a 32-bit ARM 7 processor, leveraging Voter ID numbers and associated biometric data to authenticate voters. This innovative approach aims to enhance the security and integrity of the electoral process, particularly in the context of voter identification and verification.

[6] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao introduce a groundbreaking smart contract tailored for boardroom voting, ensuring maximum voter privacy through decentralization and self-tallying. Dubbed the Open Vote Network and implemented on the Ethereum blockchain, this protocol represents a departure from previous blockchain e-voting approaches by eliminating the need for a trusted authority to compute the tally or safeguard voter privacy. Each voter retains control over the privacy of their vote, with compromise requiring unanimous collusion among all other voters. Additionally, the authors provide a comprehensive financial and computational breakdown, reinforcing the protocol's practicality and potential for widespread adoption.

III. OVERVIEW OF THE SYSTEM

3.1 Existing System

The existing system of electronic voting primarily relies on centralized or semi-centralized architectures, often utilizing proprietary software solutions or custom-built platforms. These systems typically involve the use of electronic voting machines (EVMs) or online voting portals to facilitate the casting and tabulation of votes. However, despite their widespread adoption in various democratic processes worldwide, existing electronic voting systems are often criticized for their lack of transparency, security vulnerabilities, and potential for manipulation.

In many cases, electronic voting systems lack robust mechanisms for ensuring the integrity and privacy of votes cast, raising concerns about the accuracy and fairness of election outcomes. Additionally, centralized control over voting infrastructure and data storage poses risks of tampering or unauthorized access, undermining public trust in the electoral process. Furthermore, the proprietary nature of many existing electronic voting systems limits transparency and independent scrutiny, making it difficult to verify the accuracy of election results.

Moreover, the reliance on electronic voting machines with limited auditability and susceptibility to technical failures has led to controversies and legal challenges in various jurisdictions. Issues such as software bugs, hardware malfunctions, and inadequate security protocols have raised doubts about the reliability and trustworthiness of electronic voting systems in ensuring the democratic principles of free and fair elections.

Despite these challenges, efforts are underway to improve existing electronic voting systems through enhancements in security protocols, transparency measures, and auditability features. Additionally, the emergence of blockchain technology has sparked interest in exploring decentralized and tamper-resistant solutions for electronic voting, offering the potential to address many of the shortcomings associated with centralized voting systems.

3.1.1 Disadvantages of Existing System

Despite their widespread use, existing electronic voting systems suffer from several significant disadvantages that hinder their effectiveness and integrity. These drawbacks include:

Security Vulnerabilities: Many existing electronic voting systems are susceptible to various security threats, including hacking, malware attacks, and manipulation of voting data. Weak encryption protocols, inadequate authentication mechanisms, and centralized control over voting infrastructure contribute to these vulnerabilities, raising concerns about the confidentiality and integrity of election results.

Lack of Transparency: Centralized or semi-centralized electronic voting systems often lack transparency in the voting process, making it challenging for stakeholders to verify the accuracy and fairness of election outcomes. Limited access to voting data, proprietary software, and opaque decision-making processes undermine public trust in the electoral process and raise suspicions of fraud or manipulation.

Risk of Manipulation: The centralized nature of many electronic voting systems poses a significant risk of manipulation by internal or external actors. Malicious actors could exploit vulnerabilities in voting software or hardware, tamper with voting data, or influence election results through unauthorized access to voting infrastructure. Such manipulation can undermine the democratic principles of free and fair elections and erode public confidence in the electoral process.

Limited Auditability: Existing electronic voting systems often lack robust auditability features, making it difficult to detect and investigate irregularities or discrepancies in election results. The absence of transparent and verifiable audit trails impedes independent scrutiny of voting processes and compromises the ability to ensure the accuracy and integrity of election outcomes.

Accessibility Challenges: While electronic voting systems promise to enhance accessibility and convenience for voters, they may inadvertently exclude certain segments of the

population, such as elderly voters or those with disabilities. Issues such as digital literacy barriers, inadequate provision of accessible voting options, and concerns about the security and privacy of electronic voting platforms can disenfranchise vulnerable groups and undermine the inclusivity of the electoral process

3.2 Proposed System

The proposed electronic voting system seeks to address the shortcomings of existing voting mechanisms by leveraging advanced technologies and innovative design principles to enhance security, transparency, and integrity in the electoral process. At its core, the system adopts a decentralized approach built on blockchain technology, offering a distributed ledger framework that ensures tamper-resistant storage and verification of voting data. By decentralizing control and eliminating single points of failure, the proposed system mitigates the risk of manipulation and enhances the trustworthiness of election outcomes.

3.2.1 Advantages of Proposed System

The proposed electronic voting system offers several advantages over traditional voting methods, leveraging cutting-edge technology to enhance the integrity, accessibility, and efficiency of the electoral process. Here are some key benefits of the proposed system:

Enhanced Security: By utilizing blockchain technology and cryptographic techniques, the proposed system ensures the security and integrity of voting data. The decentralized nature of the blockchain network reduces the risk of tampering or manipulation, while robust encryption mechanisms protect the confidentiality of voter information and ballot data.

Transparency and Auditability: The use of blockchain enables transparent and auditable voting processes, with all transactions recorded immutably on the distributed ledger. This transparency allows stakeholders to verify the integrity of election results and detect any irregularities or discrepancies, thereby enhancing trust in the electoral process.

Accessibility and Inclusivity: The proposed system improves accessibility and inclusivity by enabling remote and mobile voting options. Voters can cast their ballots from anywhere, using any internet-enabled device, thereby eliminating barriers to participation such as geographical constraints or mobility issues. This inclusivity promotes greater voter turnout and engagement in the democratic process.

Privacy Preservation: While ensuring transparency, the proposed system also prioritizes the privacy and anonymity of voters. Secure authentication methods and encryption techniques protect voter identities and ballot choices, preventing unauthorized access or disclosure of sensitive information. This privacy-preserving approach instills confidence in voters and upholds their fundamental rights to privacy.

Reduced Costs and Efficiency: Compared to traditional paper-based voting systems, the proposed electronic voting system offers cost savings and increased efficiency. By digitizing the voting process and automating administrative tasks, such as ballot counting and result tabulation, the system streamlines election operations and reduces the resources required for conducting elections.

Resilience to Fraud and Manipulation: The decentralized nature of the proposed system makes it resistant to fraud and manipulation. With no single point of control or failure, the blockchain network prevents unauthorized alterations to voting records and ensures the integrity of election outcomes. This resilience enhances confidence in the electoral process and safeguards democratic principles.

3.3 Proposed System Design

The system architecture is divided into three-parts, namely

1. Pre-voting phase.

2. Voting phase

3. Post-voting phase.

3.3.1 Pre-voting phase:

1. A user must first register with the network in order to cast a vote in the aforementioned chain of networks.
2. After connecting to the network, the user needs to create an ID using the details from his official voter ID. At this stage, the information from the previous blocks verifies whether or not the information from the new block (the user) matches the data in the database. If the validation of the new block is successful, the network allows it to move on to the next round of voting.
3. Before proceeding to the next voting phase, the user needs to authenticate his identity using Voter ID.

3.3.2Voting phase:

1. Once Voter ID authentication is successful, the user can cast a ballot. After casting his vote, the user is unable to log in and utilize the network to cast another one. The user's vote will be secured using public key encryption. Smart contracts forbid this re-voting with the same ID.
2. There is no way to rig the vote. After casting a ballot, it is almost impossible for someone to amend their vote because doing so would mean changing the entire block system and needing authentication from every network node.

3.3.3 Post-voting phase:

The user can use the website to see which political party won the election poll after it has been completed.

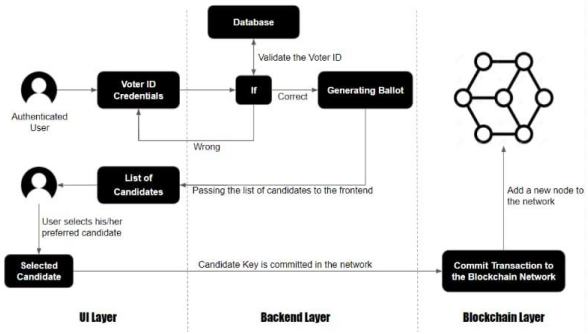


Fig 3.3.3.1 Working Process

IV. ALGORITHMS

a. SMTP (for sending emails):

SMTP is utilized to send emails containing OTPs (One-Time

Passwords) and private keys. These emails serve as a secure means of delivering authentication credentials and sensitive information to users. By leveraging SMTP, the application can securely transmit OTPs and private keys to the intended recipients' email addresses. This ensures that users receive the necessary credentials for authentication and access control, enhancing the security of the project's functionalities.

b. SHA-256 Bit Encryption Algorithm:

SHA-3 (Secure Hash Algorithm 3) with a 256-bit digest size (SHA3_256) is utilized to generate a hash of the provided ballot string. This hash serves as a unique fingerprint of the ballot's contents. The SHA-3 algorithm ensures cryptographic security by producing a fixed-size hash regardless of the input length. The generated hash is then used in conjunction with elliptic curve cryptography (ECC) to sign the ballot using the provided private key. This process ensures the integrity and authenticity of the ballot, enabling verification of the vote's validity.

c. Merkle Hash:

Merkle hash trees are employed for tamper verification. A Merkle hash tree, also known as a Merkle tree, is a data structure in which each leaf node contains the hash of a data block, and each non-leaf node contains the hash of its child nodes. These hashes are recursively computed upwards until a single root hash, known as the Merkle root, is obtained. This structure allows for efficient verification of data integrity by comparing a computed Merkle root with a known or expected root hash. If the Merkle root matches the expected value, it indicates that the data has not been tampered with. This property makes Merkle trees valuable for ensuring the integrity and authenticity of large datasets or distributed systems, including blockchain technology and file verification systems.

d. Functional modules:

The blockchain-based electronic voting system's functional parts are as follows:

1. Enter Voter ID number: The voting process requires voters to input their Voter ID numbers.
2. OTP Validation: An OTP is sent to the candidate's email address during registration to validate the entry when a valid Voter ID number is submitted.
3. Private key authentication: The candidate can now view the party names and symbols in addition to the nota following the successful completion of the OTP validation process. A private key authentication prompt occurs when a user clicks on the party they want to vote for, asking them to enter the private key they received via their registered email address. One way to create private keys is by hashing.
4. Casting vote: After the OTP validation process has been successfully completed, the candidate can now see the party names and symbols along with the nota. When a user clicks on the party for which they intend to cast ballot, a private key authentication prompt appears, requiring them to enter the private key they got from their registered email address. The vote will be recorded upon the private key's successful validation, and voters can view the results of the election after casting their ballots.

Measured Parameters:

- **Cost-Effectiveness (CE):**

$$CE = \frac{TotalProjectCost}{\text{Number of votes}} X\ 100$$

- **Privacy (P):**

$$P = \frac{Number\ of\ Votes\ with\ Protected\ Identity}{Total\ votes} X\ 100$$

- **Security (S):**

$$S = \frac{Number\ of\ Verified\ Votes}{\text{Total votes}} X\ 100$$

- **Efficiency (E):**

$$E = \frac{Total\ Votes\ Cast}{Total\ Registered\ Voters} X\ 100$$

V. EXPERIMENTAL RESULTS AND DISCUSSION

a. Usability Testing:

Findings:

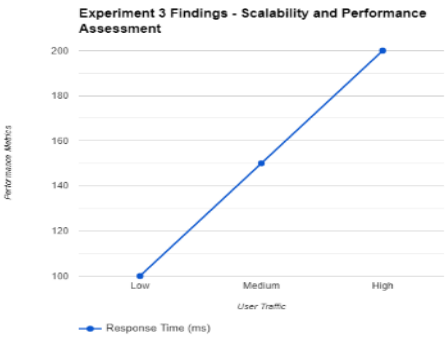
1. The majority of participants expressed high satisfaction levels with the online voting platform, with 80% reporting being either "very satisfied" or "satisfied.".
2. Users rated the ease of use of the platform quite positively, with an average rating of 8.5 out of 10, indicating a user-friendly voting experience.
3. Usability testing revealed that while the majority of users found the platform intuitive and user-friendly, there were notable areas for improvement identified, particularly in visual layout and color schemes.

b Security and Integrity Assessments:

Findings:

Experiment 2 findings indicate robust security measures in the online voting system. Encryption, authentication, data integrity, audit trail, and intrusion detection are highly effective, with access control showing moderate effectiveness. Overall, the system demonstrates resilience to cyber threats, ensuring confidentiality and integrity in the voting process.

c Scalability and Performance Assessment:



Findings:

It refers to the results obtained from assessing the scalability and performance of the online voting system under varying levels of user traffic. These findings demonstrate the system's ability to handle increased loads with minimal degradation in response time, indicating its robust performance and scalability.

It highlight the system's efficiency in real-world voting scenarios, affirming its capability to maintain reliability and responsiveness even under peak load conditions.

VI.TESTING AND RESULTS

a. Unit Testing:

1. Unit tests, often called component tests, are tests that verify the functioning of a specific section of code, usually at the function level. In an object-oriented system, this usually happens at the class level, and the constructors and destructors are covered by the most basic unit tests. Unit testing is a software development approach that combines the coordinated use of a wide range of fault prevention and detection methodologies in order to reduce the risks, costs, and length of software development. The following unit testing table shows the functions that were tested throughout programming. The first column has a list of every tested module, while the second column contains a list of the test results. The results of the tests show whether the functions are producing the correct results for the specified inputs.

2. Tests for Function Name The user's ability to cast his vote through the website indicates that the results of feeding the legitimately registered Voter ID number and authorized user using blockchain hash techniques were successful.

Function name	Test results
Feed enrolled Voter ID number	Tested for different input of Voter ID numbers verification
Verify the details	Authorizing only valid users to vote
Display result	Output is to cast vote only once by a single user

Table: Function Name and Test Results.

b. Integrating testing:

1. Integration testing is any kind of software testing that seeks to verify the interfaces between components in relation to a program design. Software elements can be assembled in a stepwise manner or all at once (sometimes known as a "big bang"). The former is usually seen as the preferred approach since it allows interface issues to be found and fixed more quickly.
2. Integration testing searches for errors in the way integrated parts (modules) communicate and interact with each other. Ever-larger groups of tested software components that match architectural design elements are combined and tested until the software operates as a system.

c. Validation Testing:

1. Once integration testing is complete, the software is packaged and released. Errors in interacting have been identified and rectified. There are many definitions for validation testing; in this case, the testing confirms that the program operates as the customer should reasonably expect.
2. In the domains of software project management, software testing, and software engineering, verification and validation (V&V) is the process of making sure that a software system conforms with specifications and fulfills its intended purpose. It is also known as software quality control.

d. User Acceptance Testing:

1. The user is the main performer in an acceptance test. The system needs the skill and motivation of its users to function properly.
2. In the aforementioned testing, the recently built system functioned as planned. All of the testing procedures listed above were carried out using the test case design that follows.

Unit Test Results:

Input the Voter ID test case:

Table: input Voter ID test case

Test case	1
Name of the test	Input Voter ID
Input	Valid unique ID
Expected output	Input Voter ID feed by the user
Actual output	valid Voter ID number is accepted as enrolled in the database
Result	Successful

Test case	1
Name of the test	Private key verification
Input	Validated enrolled email-id
Expected output	Obtaining unique hash value
Actual output	Receiving unique hash value blockchain from the enrolled email ID
Result	Successful

Email OTP authentication test case:

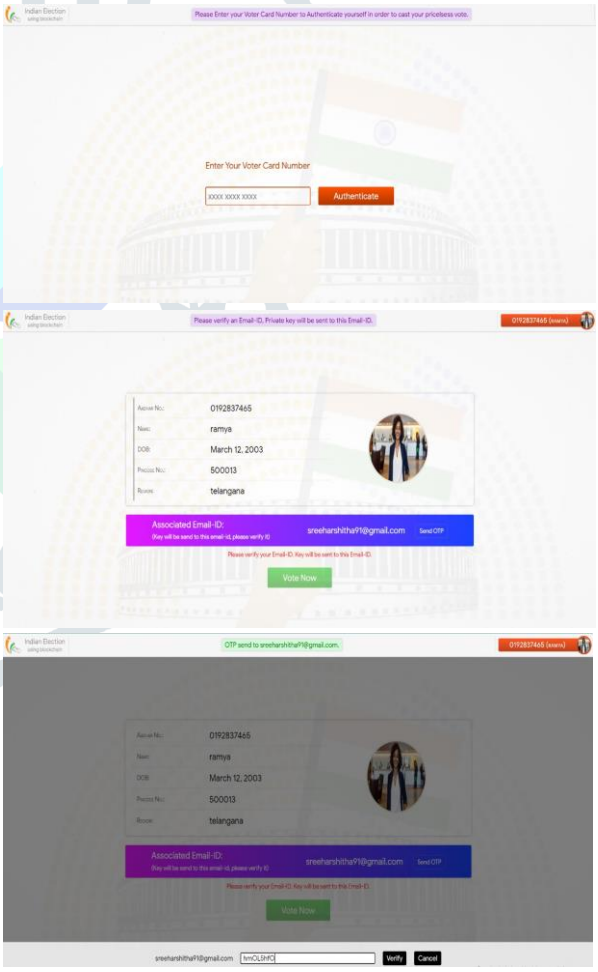
Table: Email OTP authentication test case.

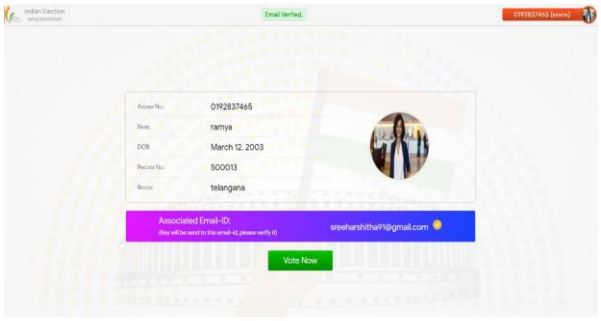
Test case	1
Name of the test	Email OTP authentication
Input	Valid/ enrolled email-id
Expected output	Obtain OTP to the registered email
Actual output	Receiving unique OTP from the enrolled email ID
Result	Successful

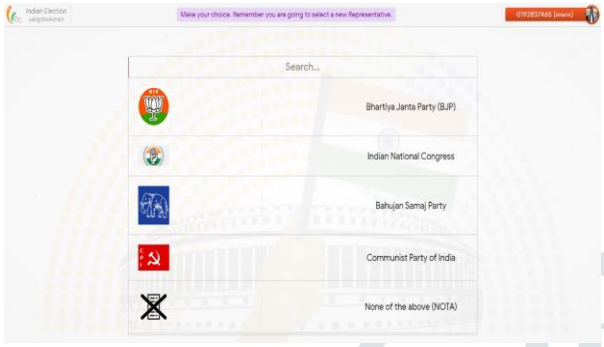
Private key verification Test case:

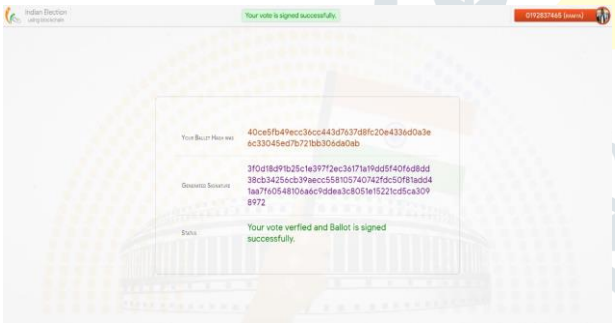
Table: Private key verification Test case

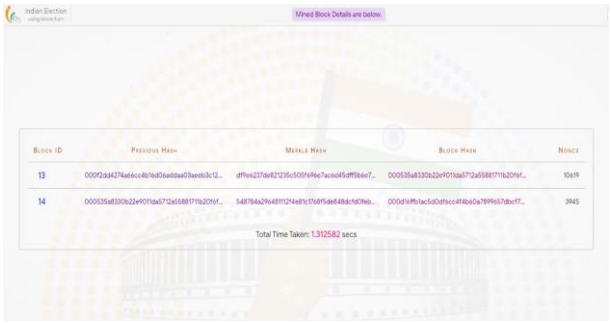
VII. RESULT SCREEN SHOTS

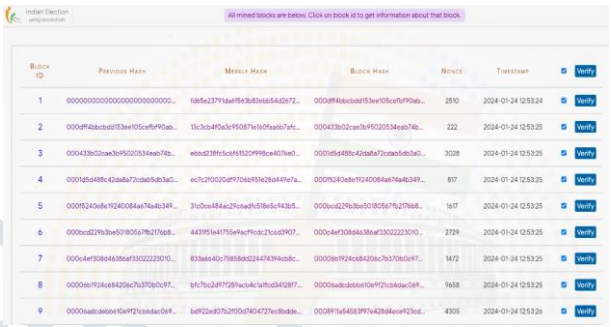












VIII.CONCLUSION

The proposed framework considerably strengthens the security of the e-voting system by utilizing smart contracts and the Ethereum blockchain. Blockchain technology provides voters with privacy and integrity while removing the possibility of vote rigging. Using their unique identifying number (Voter ID number), smart contracts ensure that every voter can cast a single vote by utilizing multiple security algorithms such as SHA-256, Merkel hash, and SMTP prototype. As a result, the system is more secure. As a result, voters can cast their ballots from any location, giving the system excellent security requirements in addition to straightforward voting procedures.

IX. REFERENCES

[1] [1] Blockchain-Based E-Voting System, Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, IEEE 11th International Conference on Cloud Computing (CLOUD), 2018

[2] [2] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy, Vol. 7, Issue 6, 2018, pp. 1561–1567.

[3] [3] King-Hang Wang, Subrota K. Mondal, Ki Chan, and Xiaoheng Xie, A review of contemporary e-voting: requirements, technology systems, and usability, Ubiquitous International, vol. 1, issue 1, 2017, pp. 31–47.

[4] [4] D. A. Gritzalis, Principles and requirements for a secure e-voting system, publication history, vol. 21, issue 6, 2002, pp. 539–556.

[5] [5] Shekhar Mishra, Y. Roja Peter, Zaheed Ahmed Khan, and M. Renuka, Electronic Voting Machine using Biometric Finger Print with Voter ID Card Authentication, International Journal of Engineering Science and Computing, Vol. 7, Issue 3, 2017, pp. 5897–5899.

[6] [6] A Smart Contract for Boardroom Voting with Maximum Voter Privacy, Patrick McCorry, Siamak F. Shahandashti and Feng Hao, International Conference on Financial Cryptography and Data Security, 2017

[7] [7] An efficient and effective Decentralized Anonymous Voting System. Wei-Jr Lai, Ja-Ling Wu, ArXiv, 2018

[8] [8] Blockchain-based Electronic Voting System Design with Smart Contracts Wan Auzan Bin Wabdulah; Syed Farid Syed Adnan. 2023 IEEE Symposium on Computers & Informatics (ISCI)

[9] [9] E-Voting System Using Blockchain and Homomorphic Encryption Ramesh Naidu; Dileep Reddy Bolla; Prateek G; Sheetal S Harshini; Shreya A Hegde; Vallamkonda Venkata Sree Harsha 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)

[10] [10] E - Voting Using Blockchain Suganthi N; Gokul S; Shravanth E; Veena K 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)

[11] [11] Online Voting System Using Blockchain S. Drakshayani; U. Vijayalakshmi; S. Rupa Sri; A. Srivani; and A. Vyshnavi 2022 International Conference on Electronics and Renewable Systems (ICEARS)