© March 2026| IJIRT | Volume 12 Issue 10 | ISSN: 2349-6002

Blockchain-Based Online Voting System with Web Portal

A. Ruchitha[1], B. Mamatha[2], B. Shirisha[3], Dr. Potu Narayana[4]
[1,2,3] *Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, India*
[4] *Associate Professor, Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, India*

***Abstract*—Traditional voting systems suffer from security vulnerabilities, lack of transparency, and risk of vote tampering. To address these challenges, the proposed research presents a Blockchain-based Online Voting System integrated with a secure web portal. The system utilizes blockchain technology to store votes as immutable and tamper-proof records, ensuring transparency and data integrity. The web portal enables secure voter registration, authentication, and vote casting through cryptographic mechanisms. Blockchain ensures that each vote is uniquely recorded and prevents duplicate or unauthorized voting. The proposed system enhances trust, security, and reliability while reducing manual effort and operational complexity. This approach provides a secure, transparent, and efficient digital voting solution suitable for modern electoral processes.**

***Index Terms*—Authentication, Blockchain, Cryptographic Techniques, Digital Voting, Online Voting System, Transparency, Web Portal.**

I. INTRODUCTION

Online voting systems are modern solutions bought on behalf of traditional voting systems. Traditional voting systems face many issues like no privacy and there are more chances of duplicate voting. It is also time consuming. Due to these issues, there is a lack of trust in the election system. With the growth of technologies, digital voting platforms are the best alternatives for improving voting systems.

Blockchain technology provides a secured and trusted system for storing the voting data. It uses cryptographic hashing and distributed ledger technology to ensure each vote is secured and cannot be duplicated or modified. By adding blockchain to web portal it ensures registered people can only vote and one user can vote only once, the vote is casted only after authentication. This process increases trust and transparency in the voting process.

Figure 1 represents the system architecture of the proposed blockchain based online voting system, including voter interaction, web portal, and blockchain network.

Based on metrics like security, data integrity, transparency and prevention of duplicate voting, the system's performance and effectiveness are measured. The proposed system (blockchain based voting system), thus improves security in elections, making sure that the vote entry is recorded, supporting digital management of elections, thereby providing a secure and a transparent solution for modern digital electronic voting applications.

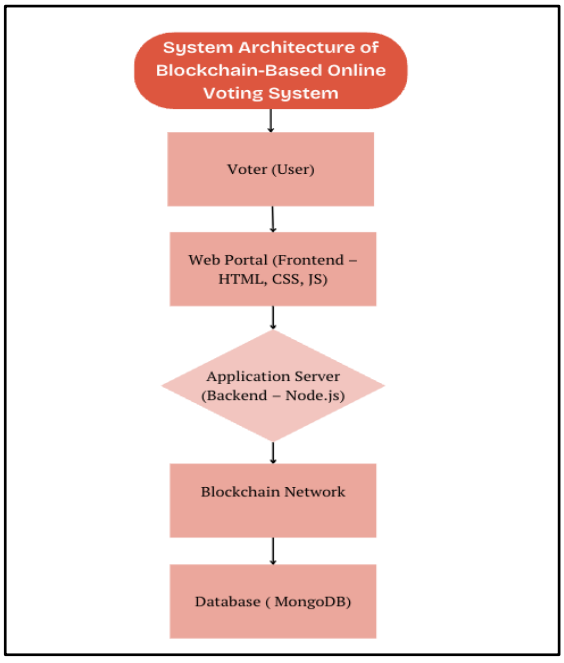

Figure 1. System Architecture of Blockchain-Based Online Voting System

II. LITERATURE REVIEW

Recent growth in blockchain technology has improved the security and transparency of electronic voting systems. The traditional voting system has many issues like duplicate voting, trust issues and no transparency in the voting system. So, in blockchain based voting system, blockchain assures that there is no tampering of votes and stores votes securely. This blockchain deals with major security issues in electronic voting system. [1]. The addition of blockchain with cybersecurity mechanisms builds system strength and reduces risk of cyberattacks and unauthorized access. [9].

Many researchers have put forward blockchain-based voting systems using smart contracts and cryptographic techniques to make sure that it is secure and voting is done automatically. Ethereum-based smart contracts enable secure vote casting, automated counting of votes, and clear result verification by removing manual interference [2], [6]. Cryptographic techniques like hybrid encryption and secure hashing algorithms improve privacy, data integrity, and protection by not giving access to unauthorised access. [10]. These approaches make sure that votes are recorded and secured and cannot be altered once stored in the blockchain.

To protect voter identity as well as to maintain system security, privacy-preserving authentication mechanisms were also explored. Also, Zero-Knowledge Proof-based (ZKP-based) methods helps in preventing duplicate voting and preserving anonymity, by allowing verification of identity in a secure manner without revealing sensitive voter information [3]. Additionally, blockchain systems along with biometric authentication and secure cryptographic hashing, improve voter verification, and also prevents impersonation attacks [5].

Decentralized blockchain frameworks like Hyperledger Fabric and permissioned blockchain networks were also implemented for improving access control, auditability, and ensure tamper-resistant system in electronic voting systems [4]. Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) are some of the consensus mechanisms which ensures efficiency in validating vote transaction, scalability, and fault tolerance in blockchain-based voting applications [7]. Also, blockchain ledger systems provides transparent audit trails, along with transaction records which can be verifiable, which helps to track votes accurately, thereby building trust in digital election processes [8]. Though the voting systems based on blockchain mechanisms have significant applications and advantages regarding security, transparency, and reliability, there are still some challenges like limitations in scalability, computational overhead, complex implementation, and transaction cost, which needs to be researched further and must be optimized [1], [7], [10]. These studies explains that blockchain technology provides a secure solution and an effective approach for modern electronic voting systems.

III.PROPOSED METHODOLOGY

Blockchain technology allows online voting in a secure and transparent manner. This is done by decentralizing of vote storage, and tamper-proof management of vote records. The proposed "Blockchain-Based Online Voting System" focuses on secure authentication of the voter, immutable recording of votes (the vote must be unmodifiable), and generating a fair and transparent results, everything, through a web portal interface. The system is designed in such a way that, it overcomes limitations and challenges like traditional way and a centralized approach in electronic voting systems, with the help of cryptographic hashing and distributed ledger mechanisms. The system's performance is evaluated based on certain parameters like security strength, duplicate vote prevention, data integrity, transparency, and overall efficiency of the system. The following subsections explain about the architecture of the proposed system, authentication mechanisms which were implemented, how blockchain was integrated, and the overall flow of the system in detail.

A. System Design and Development

The proposed system contains three key modules. They are, a web interface (like a web portal), a backend server, and a blockchain network. The web portal deals with voter registration, secured login, viewing candidates, and casting the vote. The backend server manages authentication of the user, validates the eligibility of the voter, and also connects the whole application with the blockchain layer.

Voter credentials are encrypted before storing them into the database, to enable security. Multi-level verification steps and mechanisms, like validating

unique voter ID, and proper login authentication, are implemented to prevent any unauthorized access. The proposed architecture makes sure that each voter can cast only one vote during the whole election process.

B. Security and Cryptographic Mechanisms

In this proposed voting system, security is a crucial parameter. Traditional online voting systems were exposed to centralized attacks, and manipulation of the data. To address these issues, the proposed system uses cryptographic hashing algorithms, to convert each vote into a unique hash value before integrating this or adding it to the blockchain. Each block contains the vote data, the timestamp, previous block's hash, and it's own hash value, together forming a secure chain structure. This cryptographic mechanism ensures immutability (making the data unmodifiable), which means, once the vote is recorded, it cannot be modified. This decentralized structure helps in elimination single point failures and building trust in the election process.

C. Blockchain Integration and Voting Process

The blockchain layer is responsible for storing votes in a distributed and tamper-proof manner. Once the voter casts their vote through the web interface, the backend first verifies the eligibility of the voter, and then generates a transaction. This transaction is converted into a block, and validated, after which it is appended to the blockchain. This integration of blockchain with the web interface ensures transparency, helps in tracking real-time votes, and compute or generate results securely. The proposed methodology, thus, helps in election integrity, by maintaining privacy of the voter, and scalability of the system.

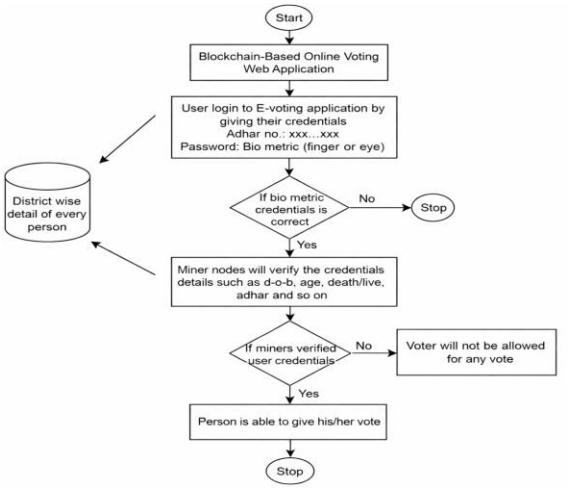

Figure 2. Workflow of Proposed Blockchain-Based Online Voting System

IV. RESULT AND DISCUSSION

The proposed "Blockchain-Based Online Voting System" was implemented in a high-performance computing environment, consisting of Intel processor (Intel Core i7), 16 GB RAM, and 1-TB SSD for proper execution in an effective manner. The system uses Python language, and for web interface, it uses HTML, CSS and JS (Javascript). For securing the vote storage and vote validation, the blockchain framework and the cryptographic-hashing mechanisms work together. The database is used for storing the credentials of the voters, and election details. The blockchain layer is used for maintaining vote records in such a way that they cannot be altered.

The performance of the proposed system is evaluated based on system-based metrics like response time, transaction processing time, along with validation of data integrity, rate of prevention of duplicate vote, and scalability rate in case of concurrent users. This makes sure that the system is decentralized and is tamper-proof storing of votes, by implementing cryptographic hashing mechanisms.

A. Performance Metrics and Evaluation

The proposed system is a blockchain-based web application, and not a machine learning model, so metrics like accuracy, precision are not applicable here. So, system-level metrics were used for evaluation.

1. Average Response Time (ART)

Average Response Time represents the average time taken between casting a vote and receiving confirmation from the system.

$$ART = \frac{\sum_{i=1}^{n} T_i}{n}$$

Where:

T_i = *Time taken for each vote transaction*

n = *Total number of vote transactions*

While testing the web-interface, 40 vote transactions were performed.

The total response time for all these transactions was approximately 112 seconds.

ART = 112 / 40

ART = 2.8 seconds
The average response time was 2.8 seconds, indicating that the system's response is effective during voting.

2. Transaction Processing Time
Transaction Processing Time is the time taken to generate a new block and append it to the blockchain.

$$TPT = T_{block\_creation} + T_{validation}$$

Where:
$T_{block\_creation}$ = *Time to generate block*
$T_{validation}$ = *Time to validate and append block*

Average block creation time was approximately 1.4 seconds, and the block validation time was 0.9 seconds.
TPT = 1.4 + 0.9

TPT = 2.3 seconds
This processing time confirms that there is no significant delay.

3. Duplicate Voting Prevention Rate(DVPR)
Duplicate Vote Prevention Rate is the ability of the system to block multiple or repeated attempts in voting.

$$DVPR = \frac{Blocked\ Attempts}{Total\ Duplicate\ Attempts} \times$$

To verify that the system prevents duplicate vote, 10 repeated voting attempts were intentionally performed.
DVPR = (10 / 10) × 100

DVPR = 100%
This confirms that the system successfully prevented multiple voting attempts.

4. Data Integrity Validation Rate (DIVR)
Data Integrity Validation helps to verify if the stored votes are unmodifiable (this is done by hash verification).

$$DIVR = \frac{Valid\ Hash\ Verifications}{Total\ Transactions} \times 100$$

The system achieved:

$$DIVR=100\%$$

All the 40 blockchain transactions are verified through hash comparison.
There weren't any mismatches in hashing, during the verification.
DIVR = (40 / 40) × 100

DIVR = 100%
This indicates that vote data was not modified or altered during testing of the system.

5. Scalability and System Stability
System Stability is the reliability of the system when users access it simultaneously or concurrently.

$$Stability\ Rate = \frac{Successful\ Transactions}{Total\ Transactions} \times 100$$

The system has a consistent effective performance, without crashing, and without any failures in the transaction.
During testing the system, 15 voters were trying to cast their votes simultaneously.
SSR = (15 / 15) × 100

SSR = 100%
The system's performance was consistent and stable, without crashes or failures, during simultaneous or concurrent execution.

TABLE 1: PERFORMANCE EVALUATION SUMMARY OF PROPOSED SYSTEM

S.No	Performance Metric	Formula Used	Observed Value
1	Average Response Time (ART)	$ART=\sum T_i / n$	2.8 seconds
2	Transaction Processing Time (TPT)	$TPT=T_{blockcreation}+T_{validation}$	2.3 seconds
3	Duplicate Vote Prevention Rate	Blocked Attempts / Total Attempts × 100	100%

	(DVPR)		
4	Data Integrity Validation Rate (DIVR)	Valid Hash Transactions / Total Transactions × 100	100%
5	System Stability Rate (SSR)	Successful Transactions / Total Transactions × 100	100%

The experimental results clearly indicate that the proposed blockchain-based voting system ensures key features like transparency, security, reliability, scalability, and efficiency. It also reduces and prevents manipulating the vote data. The evaluation results represents that the system's performance is effective during normal voting conditions as well as concurrent access (multiple voters accessing the system at the same time). The performance and the output of the system are shown in Figure 3.

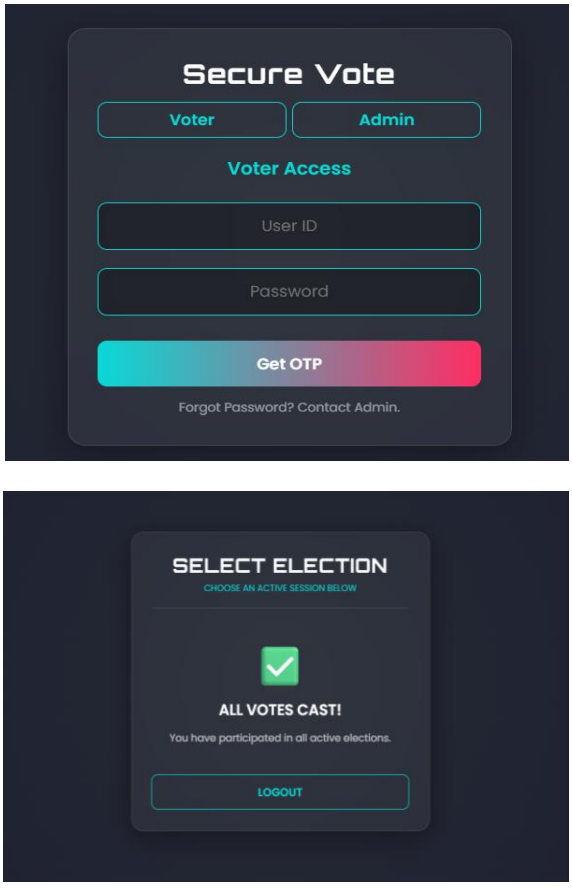

Figure 3. Web Portal Interface and Vote Verification in the Proposed Blockchain-Based Voting System

V. CONCLUSION

In conclusion, this study proposes a "Blockchain-Based Online Voting System", along with a web portal, which is secure and transparent. This overall system overcomes several limitations of traditional mechanisms for voting. Earlier conventional systems are still prone and vulnerable to security issues, and have limitations like centralized controlling, and lack of transparency. So, the proposed framework implements blockchain-based technology and mechanisms to store data securely, decentralizing the overall control, and to maintain data integrity.

The system also uses cryptographic hashing techniques along with a distributed ledger structure to prevent unauthorized access and to maintain data integrity. To prevent duplicate voting attempts, techniques like voter authentication and unique identification are implemented. The system focussed on decentralized architecture to ensure transparency of votes, to enhance trust and improve the reliability of the system in electoral processes.

The system is evaluated, and results clearly indicate that the system is secure, processes transactions efficiently, with a stable performance, even during concurrent or simultaneous access. Therefore, when compared to conventional voting systems, the proposed approach provides a secure access, and enhances tamper-resistance, improves transparency, and efficiency in operating the system. Thus, implementing blockchain technology and cryptographic hashing mechanisms in the field of digital voting is a promising solution to provide a secure, transparent and trustworthy applications for electoral voting in this modern era.

REFERENCES

[1] U. Jafar, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” IEEE Access, vol. 11, 2023.
[2] B. M. B. Pereira, “Blockchain-Based Electronic Voting: A Secure and Transparent Approach,” Electronics, MDPI, vol. 13, 2024.
[3] M. Marcellino, “Zero-Knowledge Identity Authentication for E-Voting Systems,” Lecture Notes in Computer Science (LNCS), Springer, 2022.

[4] R. Singh, “Decentralized Blockchain E-Voting Using Hyperledger Fabric,” ACM Digital Library, 2021.
[5] S. Ahmed, “Mobile Blockchain Voting System with Biometrics,” Computers & Security, Elsevier, 2022.
[6] L. Chen and J. Park, “Smart Contract Secure E-Voting,” IEEE Transactions on Information Forensics and Security, 2023.
[7] Z. Zheng, “An Overview of Blockchain Consensus Mechanisms,” IEEE Communications Surveys & Tutorials, 2023.
[8] F. Hardwick, “E-Voting with Blockchain for Transparency,” ICT Express, 2021.
[9] N. Kshetri, “Blockchain’s Roles in Strengthening Cybersecurity,” Telecommunications Policy, 2022.
[10] S. Alam, “Secure E-Voting Model Using Hybrid Encryption and Blockchain,” Springer, 2023.