ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

Blockchain-based Voting System for Secure and Transparent Elections

Pratik Arun Ravarkar[1], Tejas Prakash Kakad[2], Shreyas Avinash Nimke[3], Vedant Dipakrao Katgale[4], Shubham Ravindra Bhavir[5], Prof. Rashmi P. Bijwe[6]

[1,2,3,4,5]*Student, IT, HVPM's College of Engineering and Technology, Amravati*

[6]*Assistant Professor, IT, HVPM's College of Engineering and Technology, Amravati*

Abstract: *The Blockchain-Based Online Voting System is designed to provide a secure, transparent, and tamper-resistant platform for conducting digital elections. Traditional voting systems often suffer from issues such as lack of transparency, vote manipulation, and security vulnerabilities. To address these challenges, the proposed system integrates blockchain technology with a web-based application developed using ASP.NET and SQL Server. The system follows a multi-tier architecture where voters and administrators interact through a secure web interface. It incorporates modules such as Admin Management, Voter Authentication, Election Management, Blockchain Processing, and Audit Logging to ensure smooth and controlled operations. Each vote is treated as a transaction, encrypted, and stored within a blockchain structure where every block is linked using SHA-256 hashing, ensuring immutability and integrity of voting data. The implementation includes mechanisms for voter verification, prevention of duplicate voting, real-time vote counting, and secure result generation. Blockchain integrity is maintained through hash validation, Merkle root verification, and chain consistency checks. Additionally, audit logs are maintained for accountability and system monitoring.*

Keyword: *Blockchain, Online Voting System, SHA-256 Hashing, Digital Election, Secure Voting, Cryptography, Data Integrity, Merkle Tree, Voter Authentication, E-Governance, Distributed Ledger, Vote Encryption, Audit Logging, Web Application Security, Tamper-Proof System.*

I. INTRODUCTION

In recent years, the rapid advancement of digital technologies has transformed many sectors, including banking, education, and governance. However, the electoral process in many regions still relies on traditional voting methods or partially digitized systems, which often face challenges such as lack of transparency, security vulnerabilities, vote tampering, and delays in result generation. These issues highlight the need for a more secure, efficient, and trustworthy voting mechanism.

Online voting systems have been proposed as a solution to improve accessibility and efficiency, but they introduce new concerns related to data security, voter authentication, and system integrity. Ensuring that votes remain confidential while also being verifiable and tamper-proof is a critical challenge in designing such systems. This is where blockchain technology emerges as a promising solution due to its decentralized, immutable, and transparent nature [1].

Blockchain technology provides a distributed ledger where data is stored in blocks linked together using cryptographic hash functions such as SHA-256. Once recorded, the data cannot be altered

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

without affecting the entire chain, making it highly resistant to tampering and fraud. By leveraging these properties, blockchain can ensure the integrity and transparency of voting records while maintaining voter anonymity [2].

The proposed Blockchain-Based Online Voting System aims to address the limitations of conventional voting systems by integrating blockchain technology with a secure web-based platform. The system is developed using ASP.NET and SQL Server, following a multi-tier architecture to ensure scalability and maintainability. It includes features such as secure voter registration, authentication, election management, real-time vote casting, and automated result generation [3].

In this system, each vote is treated as a transaction and stored in a blockchain structure, ensuring that once a vote is cast, it cannot be modified or deleted. Mechanisms such as encryption, hashing, and audit logging are implemented to enhance system security and transparency. Additionally, the system enforces strict validation rules to prevent duplicate voting and unauthorized access [4].

Overall, this work focuses on designing and implementing a reliable and secure online voting system that increases trust in digital elections while ensuring efficiency, transparency, and data integrity [5].

II. LITERATURE ANALYSIS

Various researchers have significantly contributed to the development of blockchain-based voting systems by exploring different methods to enhance security, transparency, and reliability. Nakamoto (2008) laid the foundation by introducing blockchain with cryptographic hashing and distributed consensus, which later inspired secure voting applications.

Kshetri and Voas (2018) emphasized the importance of transparency and auditability in e-voting, while Hjalmarsson et al. (2018) and Hardwick et al. (2018) demonstrated practical implementations using Ethereum and token-based mechanisms to ensure vote anonymity and verification. McCorry et al. (2017) further advanced the field by incorporating zero-knowledge proofs for privacy-preserving public audits.

Yi (2019) proposed permissioned blockchain models suitable for government elections, balancing transparency with controlled access. Garg et al. (2021) highlighted existing security challenges such as device vulnerabilities and system-level attacks. Building upon these studies, the present work adopts blockchain principles within a web-based architecture to create a secure, scalable, and practical online voting system, while also identifying future opportunities for enhancing decentralization, scalability, and security.

TABLE I: LITERATURE WORK

Author & Year	Methods	Future Scope
Nakamoto (2008)	Introduced a peer-to-peer electronic cash system using blockchain with cryptographic hashing, proof-of-work, and distributed consensus.	Can be extended beyond finance to secure systems like e-voting, supply chain, and identity management.
Kshetri & Voas (2018)	Analyzed blockchain-based e-voting systems focusing on integrity, transparency, and auditability in electoral processes.	Further research on scalability and integration with government-level voting infrastructures.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

Hjalmarsson (2018)	Proposed blockchain-based e-voting using Ethereum smart contracts ensuring vote anonymity and ballot secrecy.	Improve efficiency and reduce gas costs in smart contract-based voting systems.
Hardwick (2018)	Developed a remote voting system using blockchain with token-based voting and real-time verification.	Enhance scalability and optimize transaction speed for large-scale elections.
McCorry (2017)	Implemented decentralized voting using Ethereum with zero-knowledge proofs for privacy and public auditability.	Simplify cryptographic complexity for real-world adoption and improve usability.
Yi (2019)	Proposed permissioned blockchain (Hyperledger Fabric) for national elections with controlled access and verified participants.	Integration with national identity systems for secure and scalable implementation.
Garg (2021)	Reviewed security challenges including voter device risks, DoS attacks, and identity verification issues.	Development of stronger endpoint security and multi-factor authentication systems.

III. WORKING METHODOLOGY

The working methodology of the Blockchain-Based Online Voting System is designed to ensure a secure, transparent, and efficient election process. The system follows a structured approach that integrates web technologies with blockchain mechanisms to maintain data integrity, prevent fraud, and ensure fair voting.

The methodology begins with system initialization by the administrator. The admin logs into the system using secure credentials and configures the election by defining details such as election name, schedule, and candidate information. At the same time, users register themselves as voters by submitting their personal details through an online form. These registrations are verified and approved by the administrator to ensure authenticity and eligibility.

Once the election becomes active, approved voters can log into the system using their registered credentials. The system authenticates users through encrypted password verification and checks their voting status to ensure that each voter can participate only once. After successful login, voters are presented with a list of active elections and corresponding candidates.

When a voter casts a vote, the system performs several validation checks, including verifying that the election is active, the voter is authorized, and the voter has not previously voted. Upon successful validation, the vote is processed using blockchain technology. The selected candidate information is first encrypted to maintain confidentiality. A unique hash is then generated using the SHA-256 algorithm by combining vote data, timestamp, and the previous block hash.

A new block is created containing the encrypted vote, timestamp, previous hash, and the generated hash. This block is then linked to the existing blockchain, forming a continuous and tamper-proof chain. Additionally, a Merkle root is computed for transaction verification, and a unique transaction hash is generated and provided to the voter as a receipt for future verification.

All voting activities are recorded in the database, including voter participation, transaction details, and audit logs. The system continuously maintains blockchain integrity by verifying hash consistency and detecting any unauthorized modifications.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

After the election period ends, the system automatically stops accepting votes and proceeds to result generation. Vote counts are calculated in real time, and final results are displayed in a structured format. The use of blockchain ensures that all recorded votes are secure, transparent, and immutable. This methodology ensures a reliable voting process by combining authentication, encryption, blockchain validation, and real-time processing, thereby enhancing trust and efficiency in digital elections.

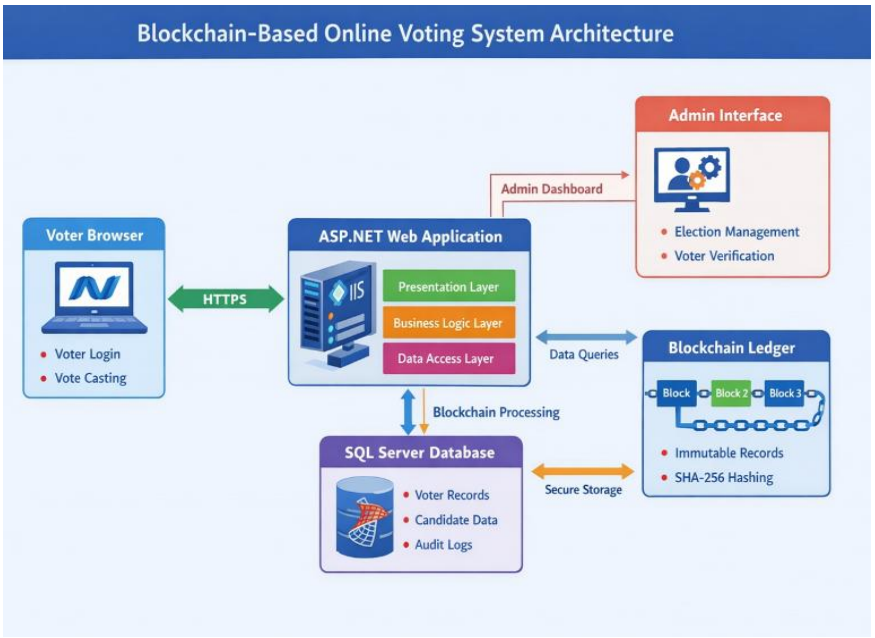


Figure 1: System Architecture

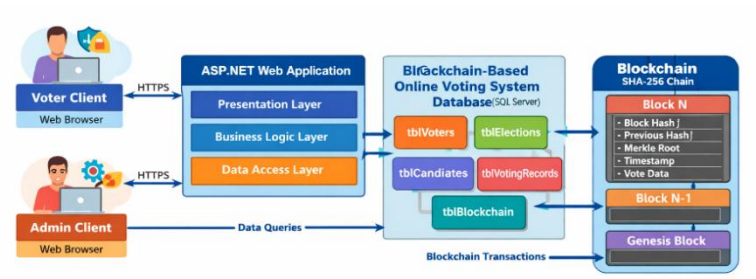


Figure 2: System Design

IV. RESULTS AND DISCUSSION

The implementation of the Blockchain-Based Online Voting System demonstrates significant improvements in terms of security, transparency, and efficiency compared to traditional voting methods. The system was tested under various scenarios, including voter registration, authentication, vote casting, blockchain validation, and result generation, to evaluate its performance and reliability. The results show that the system successfully enforces secure voter authentication using encrypted

 DOI 10.5281/zenodo.19640444

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

credentials, ensuring that only authorized users can access the voting platform. The “one voter, one vote” rule is effectively maintained through database constraints and validation checks, preventing duplicate or fraudulent voting attempts. During testing, any attempt to vote multiple times by the same user was correctly detected and blocked by the system.

The blockchain integration proved to be highly effective in maintaining data integrity. Each vote, once recorded as a block, remained immutable and resistant to tampering. The hash-based linking of blocks ensured that any modification in stored data would break the chain, making unauthorized changes easily detectable. The blockchain integrity verification algorithm consistently validated the correctness of the chain, confirming that all blocks were securely linked and unaltered.

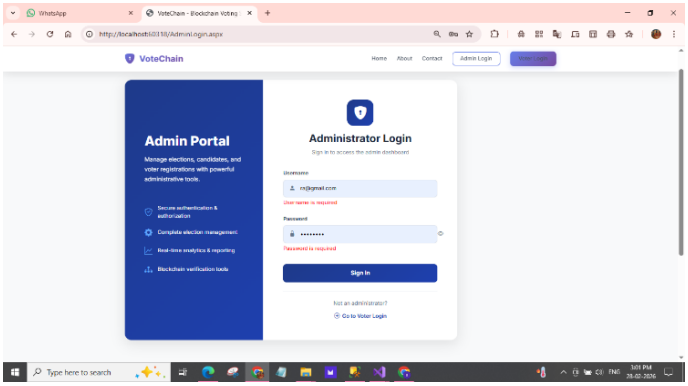
In terms of performance, the system demonstrated efficient processing of voting transactions. Vote casting, block creation, and database updates were executed with minimal delay, making the system suitable for real-time applications. The automatic vote counting feature provided instant updates, and final results were generated immediately after the election ended, eliminating the need for manual counting.

The audit logging mechanism added an additional layer of transparency by recording all significant system activities, including login attempts, voter actions, and administrative operations. This feature enhances accountability and allows easy tracking of system events for security analysis.

However, certain limitations were observed during the implementation. Since the system is built on a centralized server environment with a database-backed blockchain model, it does not fully achieve the decentralization of public blockchain networks. Additionally, scalability may become a concern when handling a very large number of voters and transactions, requiring further optimization or migration to distributed infrastructure.

Overall, the results indicate that the proposed system provides a secure, transparent, and reliable solution for digital voting. The integration of blockchain technology significantly enhances trust in the electoral process, while the web-based implementation ensures ease of use and accessibility. Future improvements can focus on increasing scalability, enhancing decentralization, and integrating advanced consensus mechanisms for even greater reliability.

Admin Sign in Page



Screenshot 4.1 Admin Sign in Page

ISSN (Online): 2583-648X

IJIRID

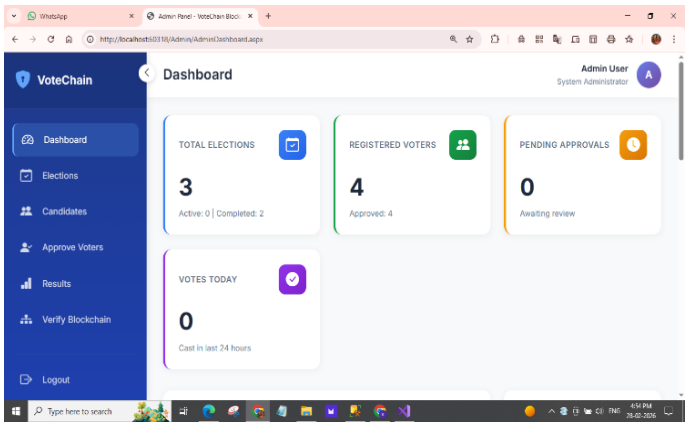
International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

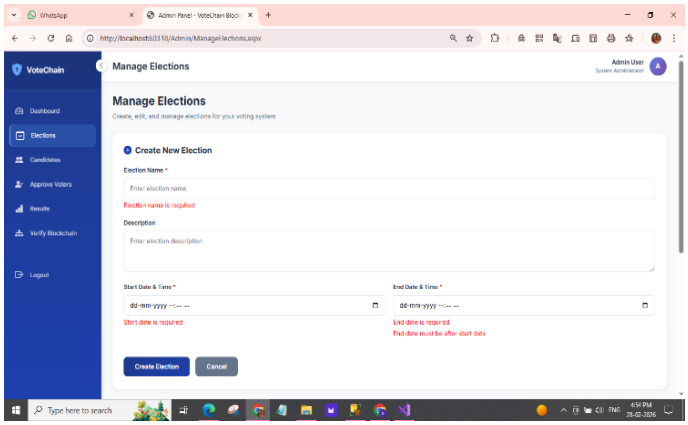
www.ijirid.in

Admin Dashboard



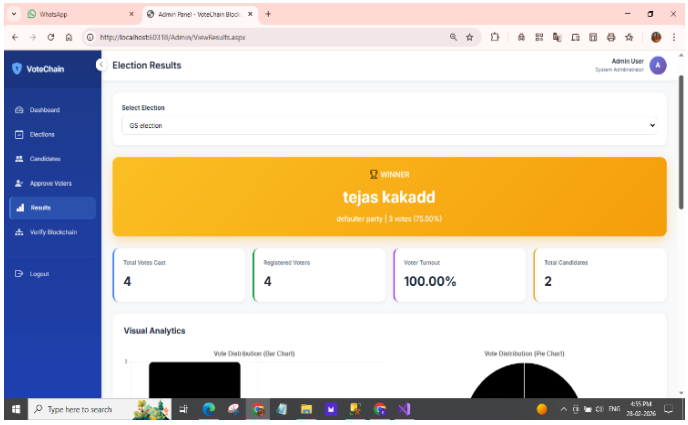
Screenshot 4.2 Admin Dashboard

Election Creation Page



Screenshot 4.3 Election Creation Page

View Voting Page



Screenshot 4.4 View Voting Page

ISSN (Online): 2583-648X

IJIRID

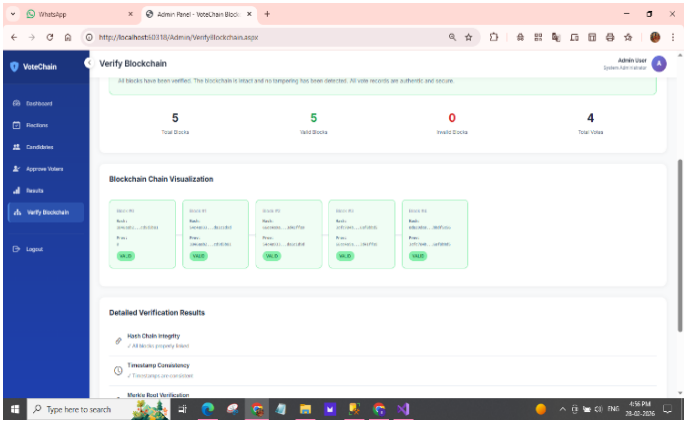
International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

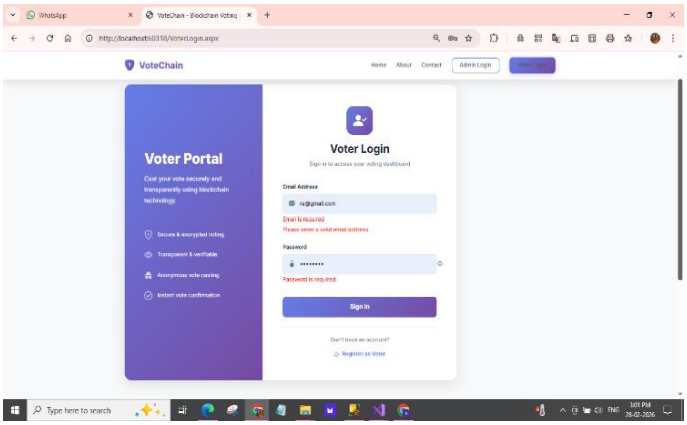
www.ijirid.in

Verify Blockchain Page



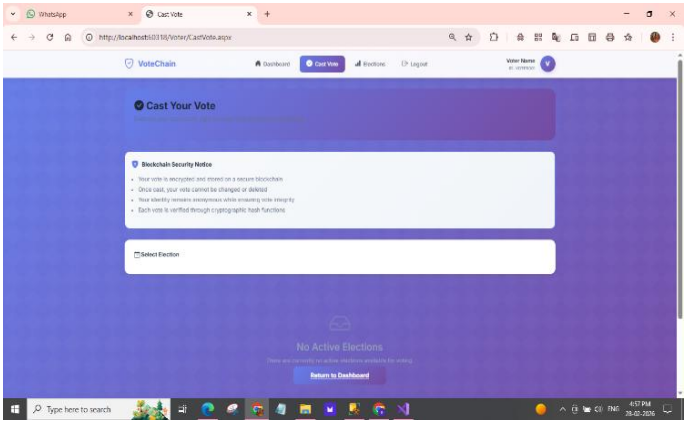
Screenshot 4.5 Verify Blockchain Page

Voter Login Page



Screenshot 4.6 Voter Login Page

Cast Vote Page



Screenshot 4.7 Cast Vote Page

 DOI 10.5281/zenodo.19640444

ISSN (Online): 2583-648X

IJIRID

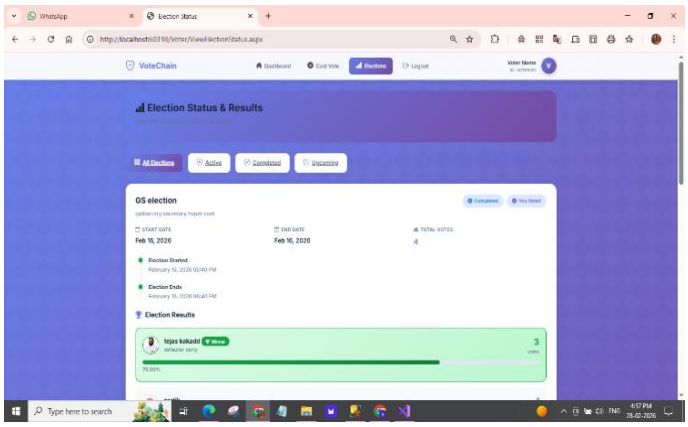
International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

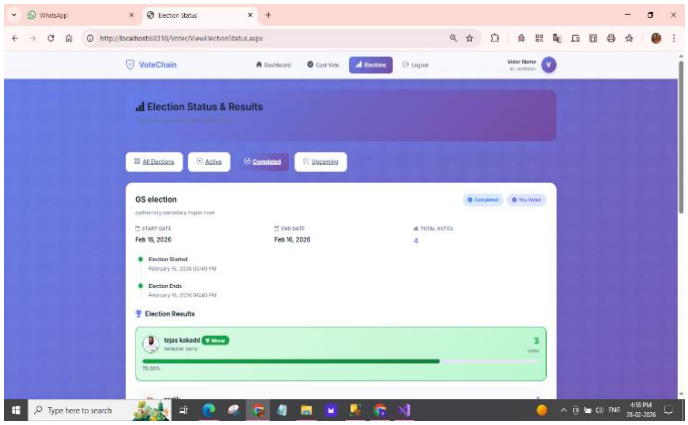
www.ijirid.in

View Election Status Page 1



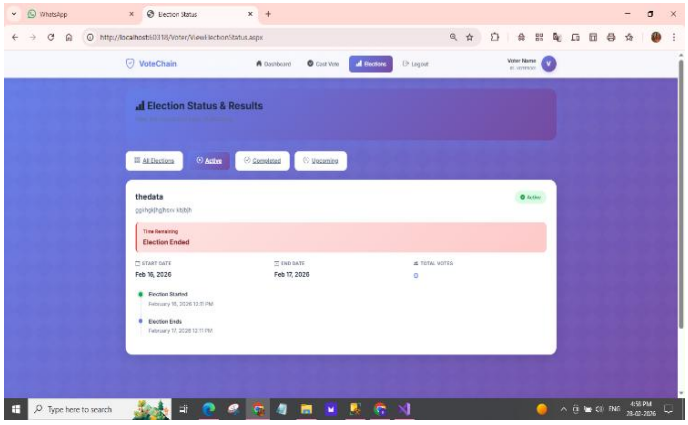
Screenshot 4.8 View Election Status Page 1

View Election Status Page 2



Screenshot 4.9 View Election Status Page 2

View Election Status Page 3



Screenshot 4.10 View Election Status Page 3

 DOI 10.5281/zenodo.19640444

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

V. CONCLUSION

The Blockchain-Based Online Voting System presented in this work offers a secure, transparent, and efficient solution for conducting digital elections. By integrating blockchain technology with a web-based application framework, the system successfully addresses major challenges associated with traditional and existing online voting systems, such as vote tampering, lack of transparency, and security vulnerabilities.

The implementation demonstrates that each vote can be securely recorded as a blockchain transaction, ensuring immutability and integrity through cryptographic hashing using the SHA-256 algorithm. The use of voter authentication, encryption techniques, and strict validation rules effectively prevents unauthorized access and duplicate voting. Additionally, the incorporation of audit logs enhances accountability and provides a clear trace of system activities.

The modular design of the system, including Admin, Voter, Election Management, Blockchain, and Audit Log modules, ensures scalability, maintainability, and ease of management. Real-time vote counting and automatic result generation further improve the efficiency of the election process while reducing human intervention and errors.

Although the system provides a robust and reliable platform, it currently operates on a centralized infrastructure, which limits full decentralization. Future enhancements can focus on integrating distributed blockchain networks, advanced consensus mechanisms, and improved scalability to handle large-scale elections.

In conclusion, the proposed system demonstrates the practical application of blockchain technology in the field of digital voting. It enhances trust, security, and transparency in the electoral process, making it a promising solution for modern e-governance systems.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

[2] Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. IEEE Software, 35(4), 95–99.

[3] Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 983–986.

[4] Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy. arXiv preprint arXiv:1805.10258.

[5] McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In International Conference on Financial Cryptography and Data Security, 357–375.

[6] Yi, H. (2019). Securing e-Voting Based on Blockchain in P2P Network. EURASIP Journal on Wireless Communications and Networking, 2019(1), 137.

[7] Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2021). A Comparative Analysis on E-Voting System Using Blockchain. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, 1-4.

[8] Microsoft Corporation. (2024). ASP.NET Web Forms Documentation. Available at: https://docs.microsoft.com/en-us/aspnet/web-forms/

[9] Microsoft Corporation. (2024). SQL Server 2019 Documentation. Available at: https://docs.microsoft.com/en-us/sql/sql-server/

[10] Microsoft Corporation. (2024). System.Security.Cryptography Namespace. Available at: https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

[11] National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS). FIPS Publication 180-4.

[12] Tanenbaum, A. S., & Van Steen, M. (2017). Distributed Systems: Principles and Paradigms (3rd ed.). CreateSpace Independent Publishing.

[13] Pressman, R. S. (2014). Software Engineering: A Practitioner's Approach (8th ed.). McGraw-Hill Education.

[14] Sommerville, I. (2016). Software Engineering (10th ed.). Pearson Education.

[15] Chart.js Contributors. (2024). Chart.js Documentation. Available at: https://www.chartjs.org/docs/

