iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73404

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Blockchain-Based Voting System for Secure Election

Abhijeet Kumar Singh
Kalinga University Campus, India

Abstract: ***Online voting is emerging as a popular trend in contemporary society. It holds significant promise for reducing organizational expenses and boosting voter participation. By allowing voting from any location with internet access, it removes the necessity for printing ballots or setting up physical polling locations. However, despite these advantages, online voting platforms are widely met with skepticism due to the introduction of new security risks. Even a single flaw can result in widespread vote tampering. Electronic voting mechanisms must be trustworthy, precise, secure, and straightforward to use during elections. Still, their implementation may be hindered by potential challenges linked to electronic voting solutions.***
Blockchain technology was introduced to help address these challenges by providing a decentralized network for electronic voting, and it is largely adopted in these systems due to its ability to deliver comprehensive, verifiable results. With its distributed architecture, resistance to tampering, and strong security features, blockchain offers an appealing alternative to traditional e-voting approaches.
This article presents a synopsis of blockchain-based electronic voting solutions. Its primary objective is to assess the present landscape of research and development surrounding blockchain-driven voting systems and to consider the obstacles they face in order to forecast future progress. The review includes a conceptual overview of the envisioned blockchain-supported e-voting platform, as well as a basic outline of the structure and principles of blockchain as they relate to voting technologies.
The findings indicate that blockchain platforms have the potential to address many of the current challenges experienced in election processes. Nevertheless, the primary concerns identified in blockchain implementations include safeguarding voter privacy and ensuring rapid transaction processing. For blockchain-based e-voting to be feasible and scalable, both secure remote access and transaction throughput must be optimized. Consequently, it was concluded that the current models require further refinement before they can be fully integrated into voting infrastructures.
Keywords: electronic voting, security, blockchain-based electronic voting, privacy, blockchain technology, voting, trust

I. INTRODUCTION

Upholding electoral integrity is vital not only for democratic countries but also for sustaining voter trust and accountability. Political voting processes are essential in this context. From a government perspective, electronic voting systems can enhance both voter engagement and trust, and can revive public interest in the electoral process. As a key method of democratic decision-making, elections have long been a significant societal issue. With an increase in actual voter turnout, the public's awareness regarding the importance of the electoral framework is also rising. The voting process determines who will act as representatives within both political entities and organizations. Democracy allows the populace to choose their leaders through casting votes. The effectiveness of this system is largely dependent on the level of trust citizens have in the election procedure. The establishment of governmental bodies to mirror the voice of the populace has become an established trend. Such entities range from student organizations to electoral districts. Over time, voting has become the fundamental mechanism through which citizens express their preferences among available alternatives.

Traditional, paper-based voting methods have played a role in bolstering public confidence in majority selection. This practice has enhanced the legitimacy of the democratic system and made it more effective in forming legislative bodies and governments. As of 2018, there were 167 democracies worldwide out of around 200 nations, with some exhibiting incomplete or mixed models. The use of confidential voting has been a longstanding approach to cultivating trust within democratic frameworks since the onset of general elections.

Maintaining confidence in the voting process is crucial. Recent findings indicate that conventional voting was not completely reliable, highlighting concerns about fairness, equal opportunity, and the accurate representation of the public's will. Such shortcomings were not fully recognized or addressed within existing governmental systems.

Globally, engineers have designed innovative voting approaches that incorporate some anti-fraud safeguards while striving to maintain the accuracy of the process. Technological progress brought forward new forms of electronic voting, which have become important but also present considerable obstacles for democratic practices. Compared to manual voting, electronic voting improves the credibility of elections. Unlike older methods, it boosts both effectiveness and honesty in the process. Its adaptability, user-friendliness, and lower cost make electronic voting prevalent in numerous decision-making scenarios. However, existing electronic voting poses risks of undue influence and data manipulation, which can undermine the fundamental principles of fairness, privacy, secrecy, anonymity, and openness in voting activities. Most current systems are centralized, authorized by a primary governing body, and subject to oversight, evaluation, and supervision a situation that creates transparency concerns in electronic elections.

Furthermore, current electronic voting protocols are typically managed by a sole administrator who oversees the entire process. This can result in incorrect outcomes if the core authority (such as an election commission) acts dishonestly, and rectifying such issues is problematic with present-day methods. Utilizing decentralized networks can serve as a contemporary strategy for electronic voting to avoid reliance on a central governing power. Blockchain technology delivers a distributed framework for both remote and digital voting. Recently, distributed ledger systems like blockchain have been applied to create such voting mechanisms, primarily due to their end-to-end auditability. Blockchain stands out as an innovative substitute for conventional electronic voting with attributes including decentralization, non-repudiation, and reinforced security. Its application spans both internal (boardroom) and broader public voting scenarios. Essentially, a blockchain is an expanding series of blocks linked by cryptography. Each segment carries a hash code, a timestamp, and transactional data from its predecessor. The architecture of blockchain is specifically designed to be tamper-resistant. Voter registration and balloting represent new domains for blockchain use; researchers in this field aim to take advantage of its transparency, confidentiality, and non-repudiation qualities that are indispensable for electoral platforms. As blockchain technology becomes more integrated with voting applications, efforts focused on safeguarding and authenticating elections through blockchains have drawn significant recent attention.

II. BLOCKCHAIN BACKGROUND

A. *Core Components of Blockchain Architecture*

These are the main architectural components of Blockchain

1) Node: A participant in the blockchain network, which can be a user or a computer; each node stores its own complete, individual copy of the blockchain's entire ledger.
2) Transaction: The fundamental unit of blockchain operations, containing recorded information and details that are processed and stored on the blockchain.
3) Block: A bundle of structured data that groups together multiple transactions; blocks are distributed across all nodes in the network for processing.
4) Chain: An ordered sequence of blocks linked together, forming the blockchain's continuous record.
5) Miners: Specialized nodes responsible for validating new transactions and appending confirmed blocks to the blockchain.
6) Consensus: The set of protocols and rules used by the network's participants to achieve agreement and validate the authenticity of transactions within the blockchain.

B. *Essential Features of Blockchain Architecture*

Blockchain architecture offers a range of advantages across various industries that utilize this technology. The following are some key features commonly embedded in blockchain systems:

1) Cryptography: Security and authenticity of blockchain transactions are maintained through advanced computational methods and cryptographic proofs exchanged among participants.
2) Immutability: Once data is recorded on the blockchain, it cannot be altered or removed, thereby ensuring the permanence of records.
3) Provenance: Every transaction within the blockchain is fully traceable, allowing for complete tracking through the ledger's history.
4) Decentralization: The distributed nature of the blockchain database enables equal access for all network participants. Control over the system is managed through consensus mechanisms at the core of the process.
5) Anonymity: Instead of typical user identification, participants in the blockchain network use generated addresses. This preserves user anonymity, especially in public blockchain platforms.
6) Transparency: The blockchain's design makes it nearly impossible to manipulate or tamper with its records, as doing so would require massive computational power, thus upholding the transparency and integrity of the entire network.

III. HOW BLOCKCHAIN CAN TRANSFORM THE ELECTRONIC VOTING SYSTEM

Blockchain technology addresses several weaknesses present in conventional election methods by making the voting process more transparent and accessible, preventing fraudulent ballots, enhancing data security, and ensuring accurate results. The integration of electronic voting with blockchain technology represents a significant advancement.

Despite the promise of electronic voting, it presents notable challenges such as the risk of system compromise, where tampering with the system might enable manipulation or misuse of vote records. These security issues are a primary reason why electronic voting has not yet been widely adopted for national elections, despite its potential benefits. Nonetheless, blockchain stands out as a practical solution for mitigating these risks.

Traditional voting platforms rely on a single central authority to process votes. If records are altered or manipulated in such a system, detecting and verifying those changes is often difficult, as the process is controlled by a single party. In contrast, blockchain eliminates central oversight; data is distributed across numerous nodes in the network. Manipulating voting data would require breaching all nodes simultaneously, which is virtually impossible. This decentralized approach not only prevents vote destruction and tampering but also enables straightforward verification of results by comparing data from various nodes.

When applied correctly, blockchain acts as a secure, decentralized, encrypted, and transparent digital ledger, resistant to tampering and fraud. The nature of blockchain allows for the establishment of an electronic voting system that is both secure and resilient against interference. Such a system requires a fully distributed infrastructure one in which control is not held by any single entity, including government bodies.

Ultimately, for elections to be perceived as free and fair, there must be widespread confidence in those elected to authority. Literature and research in this domain, along with practical trials, suggest that blockchain introduces a promising paradigm for making voting more efficient in both administration and participation. In summary, blockchain technology has opened the door to a new and improved model of electronic voting.

A. Challenges and Essential Requirements in Developing Online Voting Systems

When considering any voting platform whether it involves traditional paper ballots, electronic voting devices, or online voting there are several fundamental requirements that must be fulfilled:

1) Eligibility: The system must ensure that only authorized individuals are permitted to participate in the voting process.
2) Unreusability: Each eligible participant should be restricted to casting only a single vote.
3) Privacy: The choice made by a voter must remain confidential, inaccessible to anyone other than the individual voter.
4) Fairness: The procedure must guarantee that no one can access preliminary or partial voting results before the final count.
5) Soundness: Mechanisms must be in place to identify and reject any invalid ballots during the counting process.
6) Completeness: It is essential that all properly submitted and valid votes are accurately counted in the final tally.

IV. SECURITY REQUIREMENTS FOR VOTING SYSTEMS

1) Anonymity: Throughout the entire voting period, the system must ensure that the turnout and individual choices cannot be linked to voters. It should be impossible to associate specific ballots with voter identities within the electoral setup, thereby fully safeguarding voter anonymity.
2) Auditability and Accuracy: A robust voting platform must guarantee accuracy that the published election outcome exactly reflects the votes cast. This includes ensuring no one can alter another person's vote, all valid votes are included, and invalid ones are excluded from the tally.
3) Democracy / Singularity: The voting system is considered democratic if only those who are eligible can participate and if each qualified voter is limited to submitting a single ballot. Duplicate voting must be prevented altogether.
4) Vote Privacy: Once a ballot is cast, the system must prevent any possibility of connecting that vote to the voter's personal identity. Strong computational secrecy should protect this relationship, even as new technologies emerge over time.
5) Robustness and Integrity: The system should be resilient against attempts by groups of voters or officials to tamper with results. No participant, whether official or citizen, should be able to disrupt the election or unjustifiably dispute outcomes by alleging non-participation by others or procedural lapses.
6) Lack of Evidence (Coercion Resistance): Despite privacy safeguards, the process should be designed so that voters cannot prove how they voted even if coerced or bribed thereby deterring vote buying or intimidation.

7) Transparency and Fairness: The mechanism must ensure that no one is able to learn about intermediate or partial results prior to the official tally. This prevents using early information to unfairly influence remaining voters or to reward or punish particular electors.
8) Availability and Mobility: Voting services should remain accessible and operational throughout the polling period, and systems should enable voters to participate regardless of their physical location.
9) Verifiable Participation / Authenticity: There must be a way to confirm whether a specific voter has taken part in the election. This requirement is especially significant in jurisdictions where voting is compulsory or abstention is socially discouraged.
10) Accessibility and Reassurance: The process must assure that every eligible voter has access to a convenient polling option, with facilities readily available to those wishing to vote. Only those entitled to participate should be able to do so, and every legitimate ballot must be accurately counted.
11) Recoverability and Identification: The infrastructure should support tracking and restoration of all voting data to address potential errors, delays, or security breaches.
12) Voter Verifiability: Mechanisms should allow for auditing so participants can confirm the election was conducted correctly. This may include universal (public) verification, where anyone including independent observers and voters can review and confirm the integrity of the results. Individual voters should also be empowered to verify that their own votes have been properly recorded and included in the final count.

V. ELECTRONIC VOTING ON BLOCKCHAIN

This section outlines foundational concepts regarding electronic voting methods. Electronic voting refers to any system in which ballots are registered or counted using digital technology. Typically, electronic voting involves the utilization of both hardware and software to support the voting process. These technologies must be capable of handling various election functions, including everything from configuring the election and enrolling voters to recording votes and tallying the final results. Examples of such systems include computer terminals at polling locations, laptops, and more recently, mobile devices.

Key features required in electronic voting platforms include mechanisms for voter registration, user verification, ballot submission, and secure result calculation. Blockchain technology presents a promising way to address some of the significant challenges associated with electronic voting. Given the high-risk nature of electronic-only voting systems where breaches could have serious and widespread effects relying solely on traditional electronic solutions is often deemed impractical. However, when developed using blockchain, these networks can benefit from decentralization, openness, and consensus-driven validation, making widespread tampering theoretically unfeasible when implemented correctly. For this reason, it's important to consider the unique attributes of blockchain in the context of electronic voting applications.

Blockchain is not limited to financial uses; its architecture is versatile enough for a variety of applications, including the creation of secure, tamper-resistant online voting platforms. The concept of using blockchain to develop an incorruptible digital voting system has been gaining increasing interest.

In practice, the user experience between a blockchain-enabled voting system and a conventional electronic voting system would be largely similar. The main difference lies behind the scenes: with blockchain, each vote is encrypted and distributed across a public, decentralized ledger, rather than being stored on a central server. Every encrypted vote is confirmed through a consensus process within the blockchain, and the verified results are simultaneously recorded on all copies of the distributed ledger.

This decentralized nature means that while government authorities can monitor voting activity and results, this data is not confined to government oversight alone. The openness of the blockchain voting process ensures transparency and security votes can be independently counted by anyone with access to the ledger, but the link between voters and their choices remains protected. Thus, while both traditional electronic voting and blockchain-based voting perform similar operational tasks, blockchain introduces a fundamentally different, decentralized, and transparent organizational approach.

VI. CONCLUSIONS

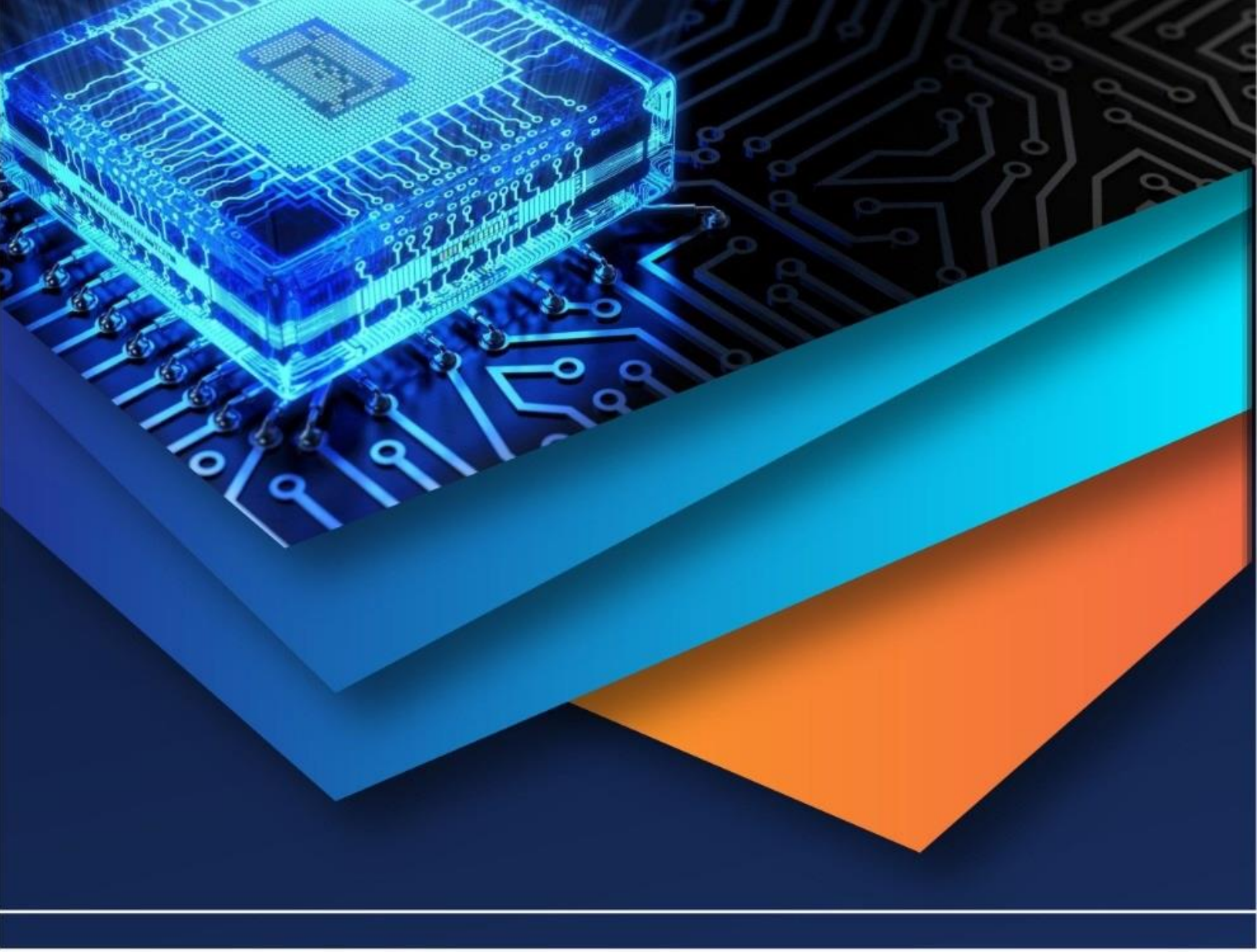
The aim of this research is to review and assess current literature on electronic voting systems that utilize blockchain technology. The article begins by introducing the foundational concepts of blockchain and its various applications, then examines the present landscape of electronic voting solutions. It goes on to identify common shortcomings in these systems and how they have been approached so far. Central to the discussion is blockchain's ability to improve reliability and security in electronic voting, current solution proposals, and possible directions for further investigation in this area. Many authorities in the field consider blockchain to be a promising basis for decentralized digital voting platforms.

One noteworthy aspect is that blockchain-based voting systems make it possible for both voters and neutral observers to access the recorded votes. However, a review of the literature shows that existing studies tend to address a recurring set of challenges. Significant research gaps remain, especially regarding certain persistent issues in digital voting. Potential disadvantages such as scaling problems, insufficient transparency, dependence on unreliable infrastructure, and lack of coercion resistance are highlighted as areas needing more thorough solutions. Since additional investigation is needed, not all risks associated with the safety and scalability of blockchain-supported voting are fully understood. The adoption of such voting mechanisms may introduce unforeseen security vulnerabilities. Furthermore, implementing blockchain demands advanced software engineering and effective management.

It is recommended that these main concerns be explored in greater detail during real-world voting trials, informed by practical experience. As a precaution, electronic voting platforms should first be piloted on a small scale before broader adoption is considered. Security deficiencies continue to affect online voting networks as well as voting hardware. To enable electronic voting over reliable and secure networks, significant security enhancements are required. Despite blockchain's promise, it is not a complete solution to all the challenges present in voting systems due to these ongoing issues. The study found that blockchain-specific complications still need attention and that several technical obstacles persist. This underscores the fact that blockchain-enabled electronic voting is still at an early developmental stage and not yet a mature solution

REFERENCES

[1] Liu Y., Wang Q. An E-voting Protocol Based on Blockchain.
[2] Shahzad B., Crowcroft J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology.
[3] Racsko P. Blockchain and Democracy.
[4] Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview.
[5] The Economist EIU Democracy Index.
[6] Cullen R., Houghton C. Democracy online: An assessment of New Zealand government web sites.
[7] Schinckus C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology.
[8] Gao S., Zheng D., Guo R., Jing C., Hu C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function
[9] Kim T., Ochoa J., Faika T., Mantooth A., Di J., Li Q., Lee Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg
[10] Hang L., Kim D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY