International Journal of Scientific Research in Engineering & Technology
Volume5, Issue6 (November-December 2025), PP: 98-104.
https://www.doi.org/10.59256/ijsreat.20250506015
www.ijsreat.com
ISSN No: 2583-1240

Secured Electronic Voting System Using Blockchain

Deepika M [1], Akash M B[2], Bharath KS[3], Chandru R[4]
[1] *Assistant Professor, Department of Computer Science and Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India.*
[2,3,4] *Department of Computer Science and Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India.*

To Cite this Article: *Deepika M [1], Akash M B[2], Bharath KS[3], Chandru R[4], "Secured Electronic Voting System Using Blockchain", International Journal of Scientific Research in Engineering & Technology, Volume 05, Issue 06, November-December 2025, PP: 98-104.*

Abstract: *Public confidence in traditional voting systems has decreased in recent years, making democratic elections more sensitive than ever. Many voters believe their rights are not fully protected, and current digital voting methods are often questioned for their lack of transparency. Since both traditional and digital systems can be vulnerable to manipulation, trust in election outcomes continues to erode. This creates a clear need for a voting method that is secure, fair, and resistant to misuse or error.*
Blockchain provides a strong foundation for such a system by delivering transparency and trust through its decentralized nature. The shortcomings of physical and digital voting approaches highlight the importance of adopting a more dependable solution that safeguards democratic values. This paper presents a blockchain-based voting framework aimed at improving security, transparency, and trust between voters and election bodies. The proposed model removes the requirement for physical polling stations and introduces a scalable digital platform that uses adaptable consensus mechanisms to support reliable and efficient elections.

Key Words: *E-polling, voting system, blockchain application, blockchain voting, E-voting, electoral system, blockchain, cryptographic hash, secure voting.*

I.INTRODUCTION

It can reduce a lot of efforts and resources invested in polling stations, specifying the areas, appointing staff, and preventing security risks at polling stations. Holding a digital election through blockchain saves money and reduces the inequity risk in the voting process. Contemporary technologies like blockchain technologies are very secure and useful if used carefully. It can make the voting system more transparent, reliable, and also enhance traceability of transactions. In the traditional digital voting system, a voting machine has been used that is connected to a centralized database.

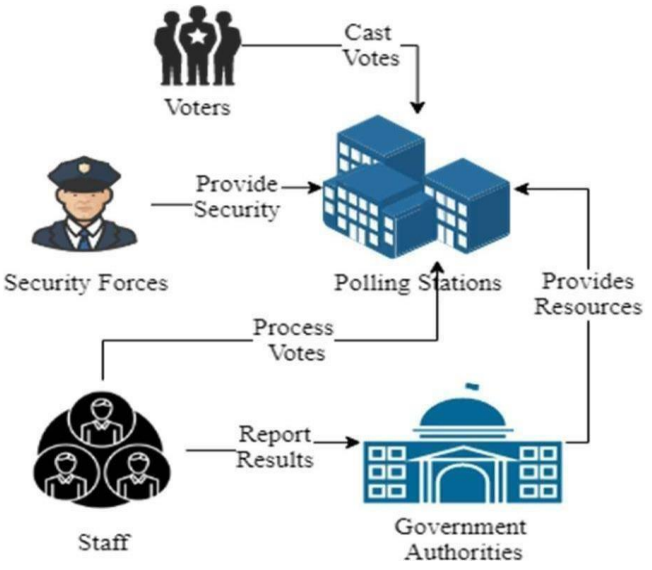
Traditional voting machines can be tampered with if someone accesses them physically, creating a single weak point that can compromise the entire system. A blockchain-based approach avoids this risk because the data is stored across many nodes, and no single person can modify it. The network constantly verifies its records, keeping the system secure even if one node is targeted.

In conventional elections, authorities may accidentally or intentionally announce incorrect results, and voters have no clear way to confirm whether their vote was counted. This often leads to mistrust and criticism, even when officials try to run the process fairly. Figure 1 shows the typical structure of these traditional systems used in many countries.

With blockchain, vote tallying becomes faster and more reliable because each node processes data independently and the results are combined automatically. Online verification through the Identification Authorities also ensures that only eligible voters take part in the election.

Tallying votes becomes more efficient in this system because calculations are performed instantly. Each node processes the information separately, and the results are combined into a single, accurate record. Voter verification is conducted online with support from the Identification Authorities, ensuring that only authorized individuals can participate. By integrating blockchain, the system prevents vote manipulation and eliminates the possibility of fake or repeated votes. Since every voter ID is valid for only one vote, the authenticity of voting records is maintained.

Blockchain also strengthens security by blocking any unauthorized attempts to access or modify data within the chain. Removing intermediaries reduces operational costs, minimizes human involvement, and decreases the chance of errors, making the voting process more reliable and resource-efficient.



II.LITERATURE REVIEW

Traditional systems of voting, both on paper and in digital format, have perennially faced the problems of transparency, security, and voter trust. A host of studies indicates significant vulnerabilities, such as vote tampering, ghost voting, human error, and centralized control that undermine democratic processes.

1. Limitations of Traditional and Digital Voting Systems

- Traditional systems highly rely on manual procedures, hence they are prone to human manipulation and counting errors.
- Digital voting machines speed things up but introduce cybersecurity risks including hacking and unauthorized access, yet it solves nothing about the central control issue.

2. Blockchain as a Solution

- Blockchain offers a decentralized, transparent, and tamper-resistant ledger, making it highly suitable for improving the trust and integrity of voting systems.
- After a vote is cast, it is encrypted and distributed across several nodes, ensuring that the record cannot be altered and can always be verified.
- The system allows only one vote per verified ID, preventing duplicate, fraudulent, or ghost voting.

3. Pilot Implementation and Hybrid Models

- The initial deployment of blockchain-based VMS is proposed along with traditional systems to validate reliability and public acceptance.
- Pilot tests in small-scale elections can help refine the system before the nationwide adoption and ensure its scalability and robustness.

4. **Comparative Studies and Global Trends**

- Research by other frameworks, including those of Pandey et al. and Farooq et al., also supports blockchain as a means for combating electoral fraud, deficiencies in transparency, and vulnerabilities within central systems.
- These studies paint a common picture: user- friendly interfaces, secure identity verification, and real-time vote tallies are what will build public trust.

5. Technological and Ethical Considerations

- While blockchain provides technical safeguards, successful implementation also depends upon regulatory support, public education, and ethical data handling.
- The literature suggests that interdisciplinary collaboration—between technologists, legal experts, and civic bodies—is essential for sustainable deployment.

III. PROPOSED FRAMEWORK FOR VOTING SYSTEM

The blockchain is mutable, unlike other programming structures where an admin can add, delete, or update the data. If that system is used for voting, then anybody having access can tamper with the system and update or delete the votes. But in the case of blockchain technology, once the node is added to the chain, it cannot be deleted or updated under any condition. In the case of attack on a node by an intruder, the corresponding nodes detect it and rebuild the damaged node, hence the chain becomes

immutable. The blockchain is decentralized, which will keep the voting system independent of any single computing node. It assures reliability under any severe condition. The main stakeholders of the proposed framework are voters, Identification Authorities (IA), and Administration Authority (AA) of election commission.

1. Voting System Architecture

In this architecture, voters access the VMS using a decentralized application (dAPP), available either as a mobile application or through a web portal. During registration, the system verifies each voter's information with the identification authority, allowing only authenticated and eligible users to participate in the election.

The system consists of several essential parts, starting with the user interface. This interface must be simple, secure, and easy to navigate, as voters enter sensitive login details here. Strong front-end security helps protect personal information, while the platform ensures equal access for every voter and provides traceability after a vote is cast.

To enroll, a voter submits their personal details, which the VMS validates by comparing them with records maintained by the identification authority. Once verified, the voter receives a unique one-time password (OTP) every time they log in to the VMS. All voter data is stored safely within the system.

2.Workflow of Proposed Model

Once a voter finishes the verification step, their details are added to the Voting Management System (VMS). The system operates on a single-chain blockchain network and is linked with the national citizen database so that every voter's identity and eligibility can be confirmed accurately.

When a vote is cast, the system generates a unique transaction tied to the voter's National ID. This transaction is then mined and permanently recorded on the blockchain. Each voter is given a "Vote Coin" in their digital wallet, and using this coin allows them to cast one vote. After the coin is used, the voter cannot vote again.

When the voter signs in with valid credentials, they are directed to the election page displaying all candidates for their constituency. Before the system allows voting, VMS checks the blockchain to see if a previous voting transaction already exists for that National ID.

- **If a transaction is found:** the system identifies that the voter has already voted, denies the request, and logs the user out.
- **If no transaction is found:** the vote request is forwarded to the miner, who will add a new node to the blockchain.

After the voter chooses a candidate and submits their vote, the transaction enters a pool. Miners review all pending transactions, filter out invalid or malicious ones through consensus with other nodes, and then add the valid vote to the blockchain as a new block. This process ensures security, transparency, and tamper-proof storage of every vote.

IV.DESIGN AND IMPLEMENTATION

In this model, a blockchain platform oversees the entire voting system, keeping voter information and election results securely encrypted on the chain. Before a vote is accepted, the system verifies the voter's nationality and checks whether they have already participated. Once the vote is submitted, its details are recorded on the blockchain, creating a transparent and easily traceable history of the voting process.

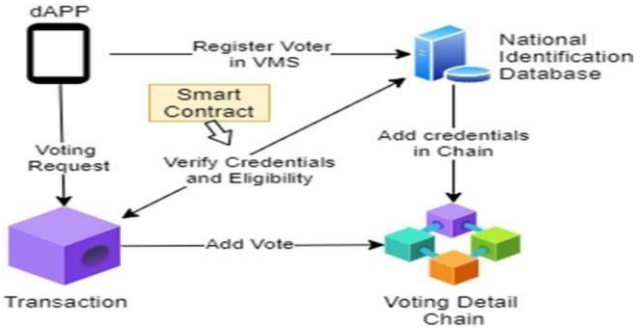


Figure 2. Smart contract incorporated in the proposed Voting Management System (VMS).

1.dAPP SETUP

The Voting Management System is built using a decentralized application (dAPP), which provides a secure and user-friendly interface for voters. By running on blockchain technology, the dAPP ensures that voter identities remain protected and that all votes are recorded in a transparent and tamper-proof manner.

Whenever a voter logs in, the system generates a new OTP, offering an additional level of authentication. Because the system is decentralized, it remains stable and dependable—every node shares the processing load. If one node becomes vulnerable or stops functioning, the others continue to operate without interruption. The faulty node can then be restored using data held by the remaining nodes, maintaining the integrity and smooth operation of the VMS.

2.Unique Voters

The system identifies each voter through their computerized National ID, allowing it to verify their information with

authorized databases and prevent identity fraud. After confirming that the voter is eligible, the system assigns them a Voting Coin. This update is recorded on the blockchain to ensure the voter cannot cast another vote. A fresh Voting Coin is needed for every voting action, which helps maintain fairness and prevents multiple votes from the same individual.

3.Election As a Smart Contract

In this model, smart contracts serve as the trusted connection between the voter and the blockchain network during every transaction. They outline the rules that govern the entire chain, and these rules must be followed by all participating nodes to ensure that each vote is stored accurately and securely.

The VMS uses a *Can-Cast-Vote* function to check whether a voter meets all eligibility requirements. Once the system verifies the voter, their details are stored for future reference. The voter is then linked to a specific voting smart contract, which selects and displays the appropriate candidates based on the voter's constituency. A vote can only be cast when both the node and the blockchain agree through consensus.

The voting smart contract shown in Fig. 5 also checks whether the voter has a valid Vote Coin in their wallet. It uses a *Cast Vote* function that requires the voter's National ID and wallet address. If the system confirms the availability of a Vote Coin, the voter is allowed to cast their vote; otherwise, the request is denied.

Each submitted vote generates a separate transaction, listed in Table 2, and the voter receives a unique Transaction ID for tracking. All transaction details are protected using cryptographic hashing to ensure data security and maintain privacy.

Overall, smart contracts provide a reliable and secure way to manage interactions within the VMS, enforcing strict rules that every node must follow to guarantee the integrity of the voting process.

4.Cryptographic Hash

Cryptographic hash conceals the data from intruders and keeps the user's identity private. While transmitting over the network, encryption protects the transaction. Only the authorized owner of the transaction can decrypt and view the content with a private key. Through SMS and email, the voter gets the address of his/her transaction, helping the voter track the vote. The voting data is saved in the blockchain using the hash value of the transaction. The voter alone, having the tracking information, has the ability to view and verify his/her voting information. The transaction gets saved securely in such a manner that the data remains unharmed and hidden.

While tracking the vote, the node is identified by the voter's public key. The voter uses his private key to view the transaction made by his wallet. The voter can only view the vote; he can never change or delete the vote once it is cast. Any user information being transferred in a transaction is encrypted by cryptography. The process of casting a vote in VMS is further elaborated in Fig. 3. It shows that while casting vote the voter adds a digital signature to the transaction. The digital signature keeps the transaction secure.

Only the voter who has the tracking information can view and verify his/her voting information. The transaction is stored in a secure manner; thus, the data remains unharmed and hidden.

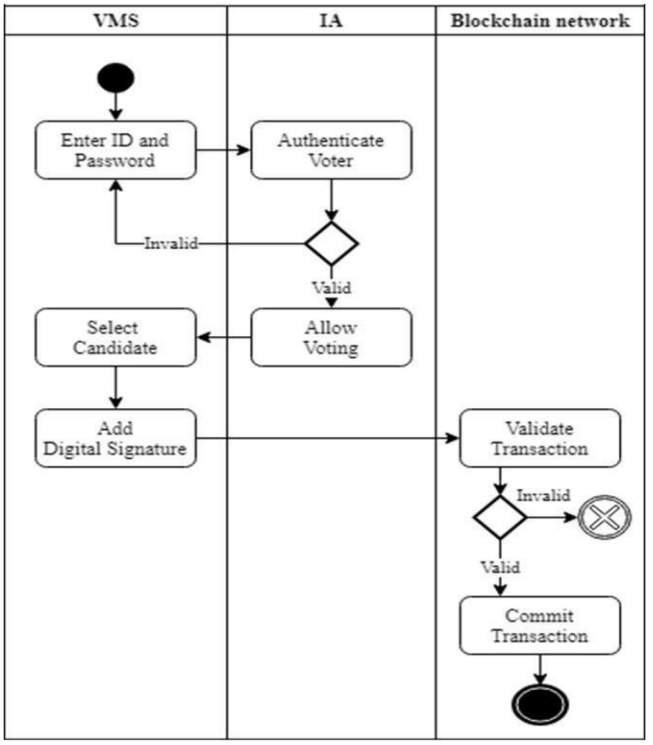


Figure 3: Process of Transaction

In a blockchain, miners can only alter the nonce value in a transaction because every other piece of data is protected through hashing. Figure 11 demonstrates how a new block is added to the VMS chain, which stores all voting transactions. The nonce is the only value a miner can modify while mining; all other fields remain locked and unchangeable.

Figure 4 breaks down the elements that make up a block, though in an actual blockchain, this information is stored in hexadecimal form. Each block is assigned a unique hash that serves as its identifier, and voters can use this hash to confirm that their vote was recorded. During the mining process, the miner repeatedly tests nonce values until the correct, or "golden," nonce is found, allowing the block to be successfully added to the chain.

Integrity and confidentiality are the salient features of block--chain technology. Locking and unlocking of messages within the blockchain are done through signatures. Thus, only the voter gets authentication to view the message. Signatures are created via the private key and message of the user. A function called a signing algorithm takes a private key and vote (message) of the voter to create a signature of that voter.

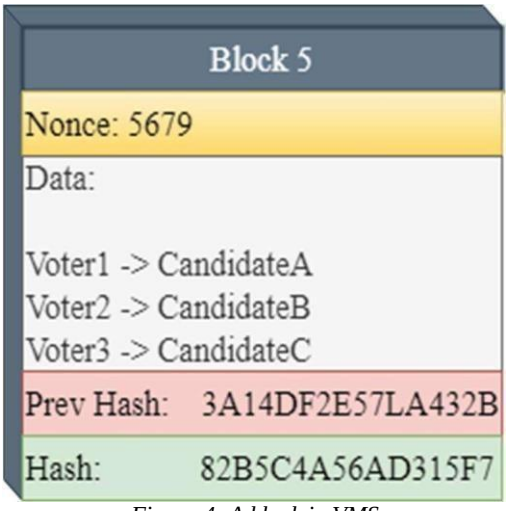


Figure 4: A block in VMS

5.Attack Prevention 51%

The 51% attack means the monopoly of 51% hash rate of blockchain. To achieve such a level of hash rate very high computational power is required. In VMS 51% of attack is prevented by two solutions. Firstly, the hash rate of each miner is pre-recorded in the system. Hash rates are monitored to check if any miner equips a 51% hash rate in a blockchain system. If such a user is detected, he is not allowed to mine during the voting process. Miners are pre-selected for the voting process. Miners are hired to mine during the voting process, under the supervision of authorities. Any external group of miners is not allowed during voting as elaborated in Fig. 5. The system is being monitored constantly while voting activity, the network blocks any malicious miner to mine block in the chain. If pre-selected miners leave the mem pool while voting activity, the system detects the activity and does not allow those miners to re-join the chain.

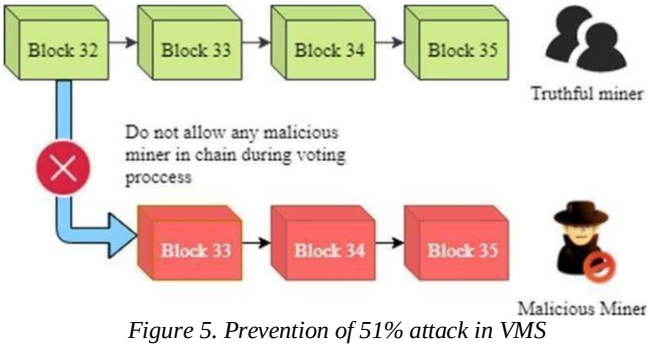


Figure 5. Prevention of 51% attack in VMS

V.PERFORMANCE APPRAISAL

This part contains the performance evaluation of the proposed framework; data is taken with real-life scenarios using Remix, a browser-based Blockchain tool. In the experimentation of the proposed model, Solidity has been used as the programming language.

A. Response Time of VMS

Response time in VMS can be determined by calculating the time taken to execute each transaction in blockchain. Fig. 6 shows response time of the system. It shows that with the increase in the votes, the response time of the VMS also increases. The blockchain is decentralized hence each node responds according to its commuting power.

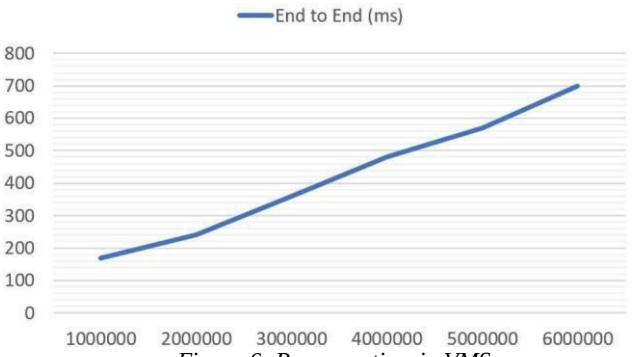


Figure 6: Response time in VMS

The growing trend of votes in the system depicts uniform growth in blockchain size. The response time increases gradually, having more nodes waiting in the memPool of miners. Flexible Consensus algorithms are applied here to keep the efficiency of the chain uniform.

B. Size of Chain

The chain size is approximately 0.004MB to 0.2MB for every 500 Blocks. As more Blocks will be added to the chain, the size keeps on increasing. In Fig. 7 uniform increment in the size of the chain is shown as the blocks are being added over time.

The increasing number of votes in the system depicts a uniform increase in the size of the blockchain. The chain has zero blocks initially; however, it increases in size since the voting process is usually 1–2 days. Therefore, latency can be an issue for a very readily growing chain. The size of the chain increases slowly when the voting process starts. After the intense voter traffic of transactions in mem Pool, the voters start to mine the transactions in the blockchain, and once the mining process starts, the size of the chain increases gradually. After successful mining of all votes in the blockchain, the tallying process starts. FIGURE 7. Behavior of size of chain.

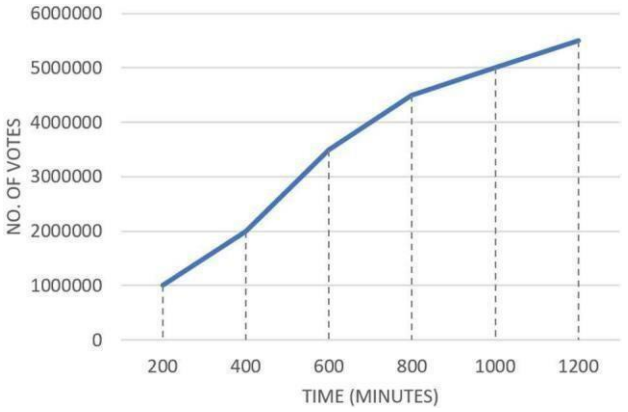


Figure 7. Behavior of size of chain

C. Latency

For the analysis of latency in the system, the time is taken for executing the transaction request has to be noted. The transaction request is triggered at a respected time that gives the latency rate of the system. As shown in Table 3 It may increase by an increase in number. of requests per second. Tallying of votes is being held on different nodes of the system during the voting process, it makes it very efficient and reduces any further processing at a singular node. Intruder nodes are blocked by using smart contract algorithms, these algorithms don't allow any incomplete transaction to hit the blockchain. The voter is only allowed to vote when all the relevant smart contracts are fulfilled. Hence, the traffic on-chain is controlled during the voting process. Latency in the chain depends on the computing power of nodes; flexible consensus algorithms keep the blockchain efficient throughout the voting activity. It reduces the latency of the system because the blockchain inclusion time of transactions is fixed.

VI.CONCLUSION

A blockchain-based solution was proposed for the voting system to build trust between government and voters to make them believe that their integrity of voting is kept safe. Blockchain-based voting makes the whole voting process more transparent and trustworthy. The amount spent on voting activity in any country is very high for the traditional voting system, whereas the proposed solution for using the blockchain voting systems makes the voting process cheaper, faster, and trustworthy.

The proposed voting system offers a secure, transparent, and dependable platform for both election authorities and voters. Performance testing of the blockchain-based VMS shows that the system continues to operate smoothly even when

handling a large volume of transactions, demonstrating its efficiency and scalability.

The goal of adopting a blockchain approach in voting is to build stronger trust between people and their government by ensuring that every vote remains protected and cannot be altered. Blockchain brings greater transparency and reliability to the election process, addressing many of the weaknesses found in traditional voting methods. Conventional elections often require significant time, cost, and manpower, whereas a blockchain-enabled system can streamline the process, making it quicker, more economical, and more trustworthy.

This technology also helps reinforce public confidence in democratic systems by providing a clear and verifiable platform on which voters can depend. The framework outlines the roles and responsibilities of election authorities within a blockchain environment, highlighting how the system improves accuracy, accountability, and trust.

Once a vote is validated, it becomes permanently recorded on the blockchain. Cryptographic hashing protects voter privacy, and the use of public and private keys ensures that only authorized entities can manage or oversee the process. The built-in traceability of blockchain further prevents unauthorized access or tampering with voting data, making the entire system more secure and resilient.

References

1. 1.S. Shah, Q. Kanhwal, and H. Mi. (2016). Block Chain Voting System. Economist.
2. Park, M. Specter, N. Narula, and R. L. Rivest "Going from bad to worse: From Internet voting to blockchain voting," Journal of Cybersecurity, vol. 7, no. 1, pp. 1–15, Feb. 2021.
3. K. M. Khan, J. Arshad, and M. M. Khan "Secure digital voting system based on blockchain technology," International Journal of Electronic Government, vol. 14, no. 1, pp. 53–63, Jan. 2018.
4. K. C. Aliprantis, F. Hjort, and H. Sato"A proposal of blockchain-based electronic voting system," Proc. 2nd World Conf. Smart Trends Secur. Sustainability (WorldS), Oct. 2018, pp. 22–27.
5. C. Barnes, C. Brake, and T. Perry Digital Voting with the Use of Blockchain Technology.Team Plymouth Pioneers – Plymouth University, vol. 14, Feb. 2022.
6. J. Huang, D. He, M. S. Obaidat, F. Vijayakumar,M. Luo, and K.-K. R. Choo"The application of the blockchain technology in e-voting: A review,"
7. M. Pawlak, A. Piekarska-Maranda, and N. Kryvinska