

# Developing a Secured Voting Sysytem Using Blockchain Trechnology

Muthukumar S<sup>1</sup>, Dr. C. Meenakshi<sup>2</sup>

<sup>1</sup>MCA, Department of Computer Application (VISTAS)

<sup>2</sup>Associate professor, Department of computer application (PG) VISTAS

DOI : <https://doi.org/10.51583/IJLTEMAS.2025.140400066>

**Abstract:** The secure voting system using blockchain technology is a transformative solution aimed at enhancing the transparency, integrity and efficiency of electoral processes. By leveraging the decentralized and tamper-proof nature of blockchain, the system ensures secure voter authentication, immutability of votes and end-to-end transparency in the voting process. Each vote is recored as an encrypted transaction on the blockchain, data integrity and preventing unauthorized alterations. The system incorporates features such as multi-factor authentication, vote tracking, and privacy-preserving mechanisms protect vote anonymity. This innovative approach address common challenges such as voter fraud, manipulation, and lack of trust offering a reliable and scalable framework for secure and transparent elections.

**Keywords:** user, voter registration, security, proof, Decentralization, Encryption, voter privacy

## I. Introduction

A secured voting system is fundamental to ensuring the integrity of democratic processes, and the use of blockchain technology has emerged as a promising solution to address the concerns of election fraud, voter manipulation and system vulnerabilities. Traditional voting system often to rely on centralized databases and intermediaries, which can be vulnerable to hacking, data breaches, and human error. In contrast, blockchain offers a decentralized, transparent, and immutable ledger system, which can significantly improve the security and trustworthiness of voting systems.

Blockchain technology ensures that votes are securely recorded and cannot be altered once they are submitted, providing a high level of transparency and accountability. Each vote is recorded as a block, and these blocks are linked together in a chain, making it virtually impossible to tamper with or delete a vote without altering the entire chain. Furthermore, blockchain allows for pseudonymous voting, where each voter's identity is protected while ensuring that the vote is cast by an eligible voter. This helps to maintain voter privacy and prevent voter fraud.

In addition to these security features, blockchain can enhance the efficiency and accessibility of the voting process. By utilizing smart contracts, voting systems can automate tasks such as vote counting, verification, and result tabulation, reducing the need for manual interventions and minimizing the risk of errors. Blockchain's decentralized nature also makes it more resilient to failures or attacks on central systems, ensuring that the voting process continues uninterrupted even in the face of technological challenges.

The adoption of blockchain technology in voting systems represents a significant step forward in safeguarding the democratic process. It has the potential to enhance voter confidence, reduce costs associated with traditional voting methods, and make elections more transparent and secure. However, while the technology holds immense promise, challenges such as scalability, regulatory compliance, and user adoption must be addressed to fully realize its potential in the electoral landscape.

## II. Literature Survey

There are lot of practices are made to introduce the variations in electronic and voting systems where different techniques and methodologies are used. Some of them guarantees the confidentiality and security to the system at some extent, still the voting information and process need to be control and manage with advanced systems that will ensures and guarantees the security and privacy of voter's and voter's information.

### Basic Voting Approach:

The systems that are developed to caste the vote by means of approach using portals and electronic devices use various encryption and decryption techniques to guarantee the secure data transaction.

### Homomorphic Encryption Technique:

Homomorphic encryption is a well-known powerful technique with many useful applications. Recently, it has been applied to the design of voting system.

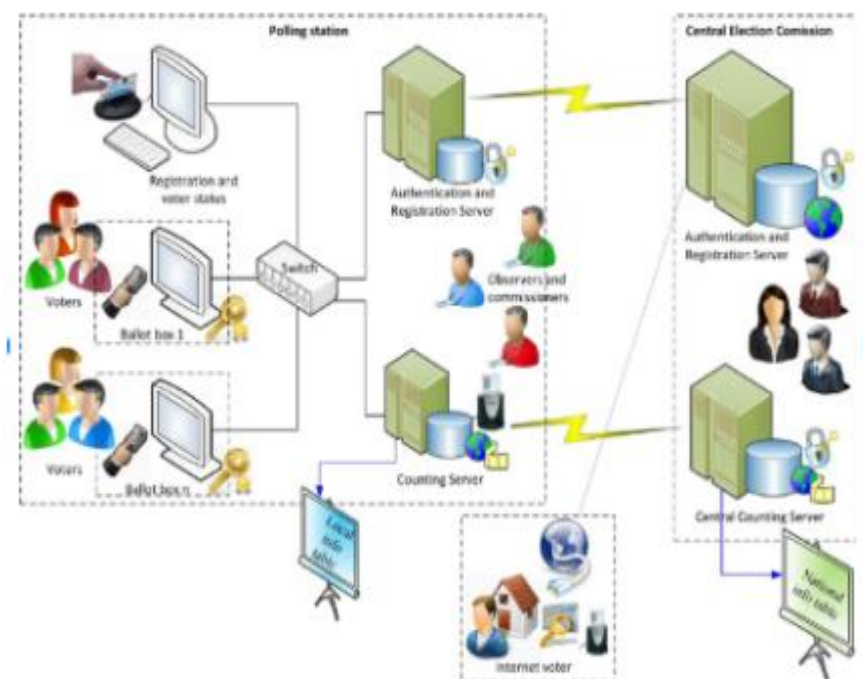
The voting system based on this encryption uses the exponential ElGamal cryptosystem. Before submission, the contents of each cast ballot are encrypted using the exponential ElGamal encryption. The additive homomorphism property of this crypto system makes it possible to tally encrypted ballots directly without decrypting them.

### Centralized architecture:

However, numbers of techniques are present to convert the data in coded format to prevent from manipulation while transferring to the network. One drawback can be discussed here that after the correct data have been stored in the database trust and security is required at substantial level. Centralized storage is inconvenient if the data is esteemed because unauthorized access and attack by hackers will challenge the system in terms of reliability.

Previous models and architectures are used with help of centralized architecture approach. That may cause ethical and security problem. Collecting the data at a centralized location we take the data at the risk. It can be controlled unfairly. So, fair framework overcomes this problem of storing information to the distributed format with the help of blockchain. Blockchain is distributed ledger that stores all processed transaction in chronological order.

Traditional databases are maintained by a single organization, and that organization has complete control of the database, including the ability to manipulate with the stored data, to censor otherwise valid changes to the data, or to add data fraudulently. For most use cases, this is not a problem since the organization which maintains the database does so for its own benefit, and therefore has no motive to falsify the database's contents; however, there are other use cases, such as a financial network, where the data being stored is too sensitive and the motive to manipulate it is too enticing to allow any single organization to have total control over the database. Even if it could be guaranteed that the responsible organization would never enact a fraudulent change to the database (an assumption which, for many people, is already too much to ask), there is still the possibility that a hacker could break in and manipulate the database to their own ends.



**Fig 1: Centralized Architecture of Voting System**

### III. Voting Background And Requirements

voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010). Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system's usability can be increased remarkably.

More recently, distributed ledger technologies such as blockchain have been used to achieve evoting systems primarily due to their advantages in terms of end-to-end verifiability. With properties such as anonymity, privacy protection and non-repudiation, blockchain is a very attractive alternative to contemporary voting systems.

### Process of Voting System

A secured voting system is a set of rules used to determine the results of an election. you can vote only if you appear in the voter list (also known as Electoral Roll) voters can also find information on polling booths.



**Fig 2: Election Process**

#### **Voting Requirements and Compliance:**

The system leverages cryptographic properties of blockchain to achieve privacy of a voter. More specifically, as voter is registered into the system, a voter hash is generated by blockchain which is the unique identifier of a voter into the blockchain, and is protected from misuse due to collision resistance property of the cryptographic hash. Due to this, the traceability of a vote is also non-trivial thereby protecting the voter when under duress.

**Privacy** - Keeping an individual's vote secret

**Eligibility** - Allowing only registered voters to vote, with each such voter voting only once.

**Receipt Freeness** - Voters should be unable to prove to a third party that they voted in a particular way.

**Convenience** - Voters must be able to vote easily, and everyone who is eligible must be able to vote.

**Verifiability** - The ability to trust the vote tallying process.

#### **Related Works:**

In (Kayas & Yung, 2002), a self-tallying voting system is proposed that does not require any trusted third parties for vote aggregation and any private channel for voter-to-voter privacy. The proposed protocol involves extensive computation. In (Hao et al, 2010) a two round protocol is proposed that computes the tally in two rounds without using a private channel or a trusted third party. The protocol is efficient in terms of amputation and bandwidth consumption but is neither robust nor fair in certain conditions (Dalia et al, 2012).

#### **Proposed System:**

The proposed Secure Voting System leverages blockchain technology to ensure a transparent, tamper-proof, and decentralized voting process. Unlike traditional electronic voting systems, which are vulnerable to hacking and fraud, this system records each vote as a secure, immutable transaction on a blockchain network, eliminating the risk of manipulation.

Using smart contracts, the system automates voter authentication, vote recording, and result tallying, ensuring a secure and verifiable election process. Each voter receives a unique cryptographic key to cast their vote, which is encrypted and stored on the blockchain. Since blockchain is decentralized, votes cannot be altered or deleted, making the system fully transparent and resistant to cyber threats.

#### **Module Description:**

**Voter Authentication Module:** Ensures that each voter is authenticated using their unique cryptographic.

**Voting Module:** Records the votes in real-time and adds them as transactions to the blockchain.

**Blockchain Network:** Utilizes nodes to ensure decentralization and immutability of the voting data.

**Smart Contracts:** Automates key processes like voter verification, vote casting, and result tallying.

**Results Dashboard:** Provides a transparent and real-time view of election results without revealing.

| TABLE DESIGN |                                                                              |                                                                                                                 |
|--------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Table Name   | Fields                                                                       | Description                                                                                                     |
| Voter        | Voter id<br>(primary key)<br>Name, Age<br>Address<br>Unique key              | Stores voter information including a unique cryptographic key used each voter.                                  |
| Vote         | VoteID (primary key), voter ID (Foreign Key) Candidate ID, Timestamp         | Records the vote details, ensuring each vote has a unique identifier and linking it to the voter and candidate. |
| Candidate    | Candidate ID, (primary key), Name, Party, Election ID                        | Stores information about the Candidates participating In the election.                                          |
| Election     | Election ID (primary key), Election Name, StartDate, End Date                | Contains data about various elections, their duration, and other members.                                       |
| Blockchain   | Transaction Hash (primary key), Block Number, Previous Hash, Data, Timestamp | Stores the blockchain log data, ensuring integrity and transparency of vote transactions.                       |

#### Form Design For Voting System:

**Login Form:** Authentication for voters using their unique cryptographic key and credentials.

Fields: Voter ID, Password, Captcha

**Voting Form:** Enables voters to cast their vote.

Fields: Election Selection (Dropdown), Candidate Selection (Radio Buttons), Submit Button

**Admin Form:** For election administrators to add candidates, manage elections, and monitor blockchain log

Fields: Election Name, Candidate Name, Start Date, End Date, etc.,

### Flowchat of Voting System:

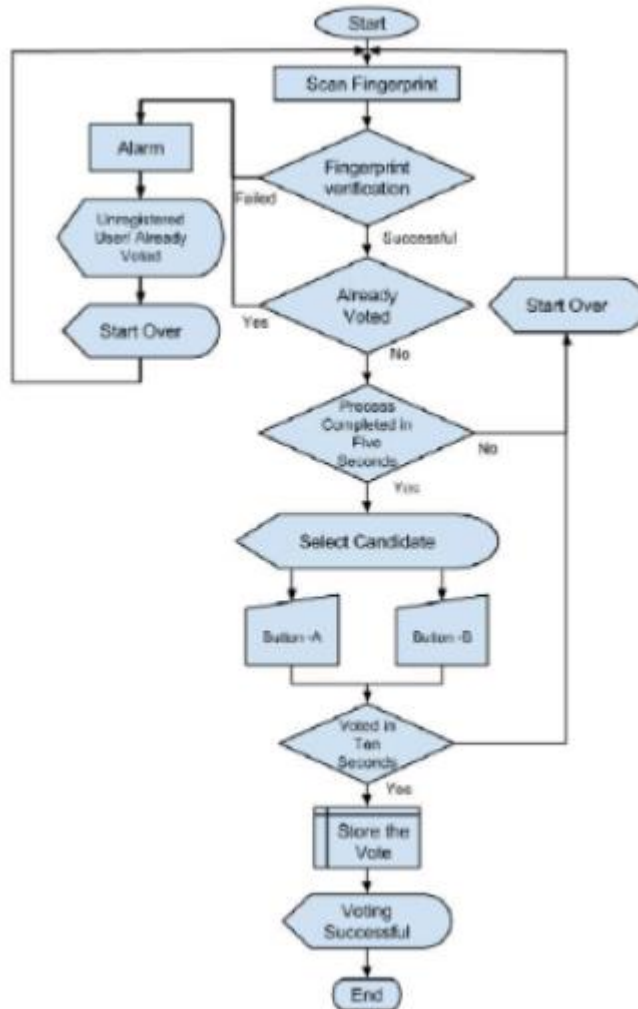


Fig 3: Flow Chat

## IV. Implementation and Evaluation

### Implementation:

The implementation of the proposed system has been carried out within a controlled environment with a web-based application created to serve as the frontend application enabling the users to interact in a convenient manner.

To create a private blockchain for this application which is used for recording the voting transactions

### Evaluation and Experimentation

The primary objective of evaluation was to assess the performance of the system in view of the voting system requirements presented in section 2 and to identify any considerations with regards to its application in a real-world scenario.

The experimentation consisted of multiple steps i.e. conducting multiple transactions, verification of transactions, mining transactions into blockchain, reflection of the changes made in the public ledger to all the nodes in the network and the usability of the system.

## V. Conclusion And Future Work

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paperbased systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to voting. This paper has presented one such effort which leverages benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to voting.

In continuation of this work, we are focused at improving the resistance of blockchain technology to ‘double spending’ problem which will translate as ‘double voting’ for voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction however successful demonstration of such events have been achieve which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for voting systems will be crucial to achieve an end-to-end verifiable voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure.

**Reference**

1. Adida, B.; ‘Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium, ser. SS’08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335{348}.
2. Adida B. and Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting, in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES ’06. New York, NY, USA: ACM, 2006, pp. 29-40.
3. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). Star-vote: A secure, transparent, auditable, and reliable voting system, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX.
4. Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). Bingo voting: Secure and coercion- free voting using a trusted random number generator, in Proceedings of the 1st International Conference on voting and Identity, ser. VOTE-ID’07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.