# E-Voting System using Blockchain Technology and Fingerprint Authentication

**Mr. Ganesh Tambe, Mr. Omkar Dambale, Ms. Rutuja Pawar,**
**Ms. Arati Kolpe, Mr. Vijay Sonawane**
Department of Computer Engineering
JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Maharashtra, India

**Abstract:** *Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on evoting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.*

**Keywords:** Security and Protection, Internet Voting System, Voter Password, Visual secret sharing

## I. INTRODUCTION

With digitization in millennial years, electronic voting systems have been used in many countries for their general elections as well. In 2005, Estonia become the first country to have general public election nationwide through e-voting. The same was adapted by various European countries like Switzerland and Norway. A major issue faced for these elections was maintain its spree with traditional ballot system to give voter with privacy of vote and maintain integrity of vote after casted. The main challenge was that the vote must not be tampered and changed under any influence. However, this technique was not able to provide with total animosity and many agencies were able to identify and intercept the casted. Blockchain is secure and safe way for same system to make more reliable and trustworthy From the dawn of democratically electing candidates, the voting system has been based on pen and paper scheme. Replacing the traditional pen and paper scheme with a new election system is a new idea for researchers. An E-voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with.

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences

changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes

DOI: 10.48175/IJARSCT-7869

### 1.1 Blockchain

A blockchain may be a form of distributed ledger technology (DLT) that consists of a growing list of records, known as blocks, that area unit firmly joined along victimization cryptography. every block contains a cryptanalytic hash of the previous block, a timestamp, and group action information (generally pictured as a Merkle tree, wherever information nodes area unit pictured by leaves). The timestamp proves that the group action information existed once the block was created. Since every block contains info regarding the previous block, they effectively kind a sequence (compare joined list information structure), with every further block linking to those before it. Consequently, blockchain transactions area unit irreversible in this, once they're recorded, the info in any given block can not be altered retroactively while not fixing all resulting blocks. Blockchains area units are usually managed by a peer-to-peer (P2P) network to be used as a public distributed ledger, wherever nodes conjointly adhere to an accord algorithmic program protocol to feature and validate new group action blocks. though blockchain records don't seem to be unalterable, since blockchain forks area unit potential, blockchains are also thought-about secure by choice and exemplify a distributed ADPS with high Byzantine fault tolerance.

### 1.2 Blockchain Features

#### A. Suburbanized

The network is suburbanized which means it doesn't have any governing authority or one person taking care of the framework. Rather a gaggle of nodes maintains the network creating it suburbanized.

#### B. Immutableness

Immutability means that one thing can't be modified or altered. this is often one of the highest blockchain options that facilitate making sure that the technology can stay because it is – a permanent, unalterable network.

#### C. Increased Security

As it gets obviates the requirement for a central authority, nobody will simply merely modifier any characteristics of the network for his or her profit. victimization cryptography ensures another layer of security for the system.

#### D. Distributed Ledgers

Usually, a public ledger can offer each info a few dealing and therefore the participant. it's all go in the open, obscurity to cover. though the case for personal or united blockchain may be a bit completely different. But still, in those cases, many of us will see what extremely goes on within the ledger.

## II. LITERATURE SURVEY

Innovation in digital technology has helped new millennial generation with many new things. Traditional Use of Paper for electoral process is changed with advent of digital technology. More conventional method through technology is implemented. But as the change is implemented more threat towards security and data integrity of casted vote is considered in this conventional method which is done when Offline. The system which can allow decentralize system to come together with entire database which is owned by many users as well maintain data integrity for system can be embraced by Block chain technology as one of the solutions.[1]

Amongst the young tech savvy generation there is lack of casting vote, this E-voting is a perfect solution for samevoting Block-Chain technology is one of the solutions for e-voting to become more transparent and open. Block Chain technology can be used in various fields but now Block chain technology is not in in its full potential.[2]

Since 1970's electronic voting is used as it gives benefits over the use of paper-based system in accuracy and reduced errors. With advent of block chain technologies, major initiatives are taken to check the feasibility of same in use of e-voting. The proposed approach is used with Multi-chain and in-depth evaluation of approach [3].

## III. EXISTING SYSTEM

Electronic voting is the standard means of conducting elections using Electronic Voting Machines(EVMs) inIndia. The system was developed and tested by the state-owned Electronics Corporation of India and Bharat

DOI: 10.48175/IJARSCT-7869

Electronics in the 1990s. They were introduced in Indian elections between 1998 and 2001, in a phased manner.
Prior to the introduction of electronic voting, India used paper ballots and manual counting. The paper ballots method was widely criticised because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots. The printed paper ballots were also more expensive, requiring substantial post-voting resources to count hundreds of millions of individual ballots. Embedded EVM features such as "electronically limiting the rate of casting votes to five per minute", a security "lock-close" feature, an electronic database of "voting signatures and thumb impressions" to confirm the identity of the voter, conducting elections in phases over several weeks while deploying extensive security personnel at each booth[1]have helped reduce electoral fraud and abuse, eliminate booth capturing and create more competitive and fairer elections. Indian EVMs are stand-alone machines built with once write, read-only memory.[4]The EVMs are produced with secure manufacturing practices, and by design, are self-contained, battery-powered and lack any networking capability. They do not have any wireless or wired internet components and interface. The M3 version of the EVMs includes the VVPAT system.

## IV. PROPOSED SYSTEM

As the general public look from far off, there's the likelihood of obtaining Counterfeit or pretend product. This preooter tends product affects the cliefooternt further than the name. They have to face major losses from this case. there's no right answer before managing this downside. As simply derived barcodes there's no guaranteed system, or an honest answer to differentiate counterfeit products from real products. Blockchain is the most promising technology rising in recent years which will facilitate to unravel of that form of downside. Blockchain Technology may be accustomed monitor and keeping track of shipped products so that users solely get the correct product. the most purpose of the project was to bring transparency concerning the merchandise throughout client getting and facilitate customers to envision if the merchandise they're shopping for is original or counterfeit simply.

### 4.1. Objectives of System

The idea of this project came into existence thanks to the rise of counterfeit products. The objectives of this project are:

- Taking bio-metric for verification and Identification.
- Using SHA256 for security.
- Save manpower

## V. SYSTEM ARCHITECTURE

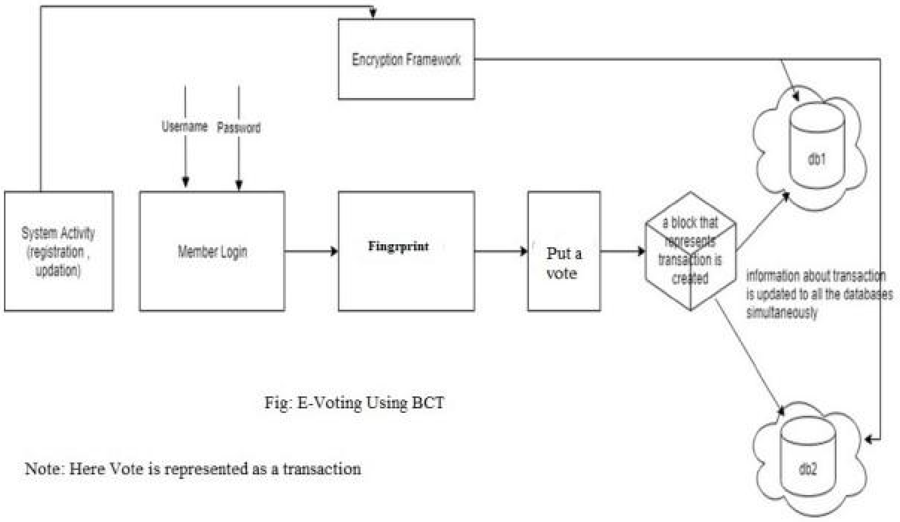
Encryption Framework
Username
Password
System Activity (registration , updation)
Member Login
Fingrprint
Put a vote
a block that represents transaction is created
db1
information about transaction is updated to all the databases simultaneously
db2
Fig: E-Voting Using BCT
Note: Here Vote is represented as a transaction

**Figure 3:** Proposed System Architecture

Whenever any transaction will occur in the system, the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the block's hash must be changed. Such multiple copies are maintained at different servers, which will assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the voting system.

### 5.1. Project Modules

- **Admin**: admin can add candidate, voter, ward and election. He/she can perform update delete operation and declared result also.
- **Fingerprint**: Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using Fingerprint.
- **User**: Voter can vote only if he/she logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using Fingerprint scheme.
- **Blockchain**: Block chain is a distributed database that stores data records that continue to grow, controlled by multiple entities. Block-chain (distributed ledger) is a trustworthy service system to a group of nodes or nontrusting parties, generally block chain acts as a reliable third party to keep things together, mediate exchanges, and provide secure computing machines.

### 5.2. Algorithms Used

SHA-256 rule the SHA-256 rule is one flavor of SHA-2 (Secure Hash rule 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 could be a proprietary cryptographical hash operation that outputs a price that's 256 bits long.

1. Sha-256 rule is employed in the blockchain to induce a continuing hash of 256 bits each time. This rule is additionally a part of secret writing technology. So, currently, let's see how this rule works:
2. In the figure you'll be able to see the example of the rule. during this, there's some information known as IV which is 256 bits. currently, the input we tend to get is going to be within the massive. So, we break it in the size of 512 bits.
3. As the input can perpetually be not an ideal multiple of 512 bits, So, some parts of the input are going to be left. 4. to the current left input we tend to do a cushioning concatenate the input with ten bits before it. currently, our input is ideal multiple, therefore we will proceed additional.
4. This output 256 bit is once more united with 512 bits input from block B2.
5. Again, a press operation starts and offers the final 256-bit output, which we tend to decision it as the hash of the input file.

## VI. CONCLUSION

The survey has been done through the way where Blockchain is used for online transaction, maintaining smart contracts and blockchains use in M2M-REP for machine to machine communication. Considering the security provided by blockchain, consideration of same for voting system is approach for this system where same security and integrity has to be maintained, Internet based voting become reliable and ensures more participation with help of blockchain. This is obtained through low cost and integrity for each vote is assured. The proposed system uses visual cryptography to provide mutual authentication for voters and election servers, Blockchain technology serves for data integrity and security.

## REFERENCES

**[1].** Ahmed Ben Ayed, "A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.[1]

**[2].** Rifa Hanifatunnisa, Budi Rahardjo, "Block-chain Based E-Voting Recording System Design",IEEE 2017.[2]

**[3].** Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Block-chain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.[3]

**[4].** Ali KaanKoç, EmreYavuz, Umut Can Cabuk, Gokhan Dalkilic, "Towards Secure E-Voting Using EthereumBlockchain",2018 IEEE.[4]