

# E-Voting using Blockchain System

Priyanka Patil, Shweta Tandel, Dipali Kumbhar

Dept. of Computer Engineering , Mumbai University  
Datta Meghe College Of Engineering, Airoli Navi Mumbai

**Abstract** – The aim of this paper is to show that digital system using blockchain technology is very useful for voting system and also solves the problem of tampering data. E-voting that is electronic voting uses for counting a votes. Present system for election works manually , which takes a lot of effort for conducting the elections and calculate the votes. By using blockchain technology the voting system gives the better result and less efforts will be taken. For security MD5 algorithm is used in these.

**Keywords**– Blockchain, Decentralization, Distributed System, electronic voting, verifiable voting.

## I. INTRODUCTION

Election is important aspect of the democracy in all over world. Election give chance so that people can raise their voice, opinion and choose the correct person whose ideas are connect with them the most. So the election affects the society so much, the election process should be transparent to give fair decision towards people. There are many ways to do voting the most used technique is paper ballot , in which voters write their candidate name in a paper and put the paper into box and then votes get calculated. Basically one sealed box is given to all over places for voting called Electronic Voting Machine (EVM) . Once the voting done the votes in the box manually calculated in presence of official authorities . This is somewhere risky, where voter can vote two times or to make one candidate win intentionally votes can be changed ,there is always a threat of tampering a data . As EVM is found not much secured also not tampered proof , so hacking this is really simple. So in this case , along with Electronic Voting Machine (EVM) we use blockchain concept to avoid the tampering. Blockchain basically provide the security to our votes ad it is really hard to crack the blockchain security algorithm ,to tamper a data. Blockchain concept developed by a person (or group of people) using the name Satoshi Nakamoto in 2008 . blockchain is highly useful concept in the voting it allow user to connect network and for every individual voter new block is created of their vote in it with unique generated hash value ,that remains valid until data got tampered. So its strong value in cryptography implementing such technique in our voting system achieved remarkable progress in the world of election.

## II. LITERATURE SURVEY

There are lots of efforts are put in to made a variations in Evoting systems where many different technologies are used. Few of them gives guarantee of confidentiality and security to the system at some level. Still voting process needs to be handle and control with new advanced system

that will give assurance to voter about his vote and voters personal information. Online voting system powered by aadhar authentication.

## III. BLOCKCHAIN

Blockchain technology was first used within Bitcoin and is a public ledger of all transactions. A blockchain stores these transactions in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a linear, chronological order to the blockchain.

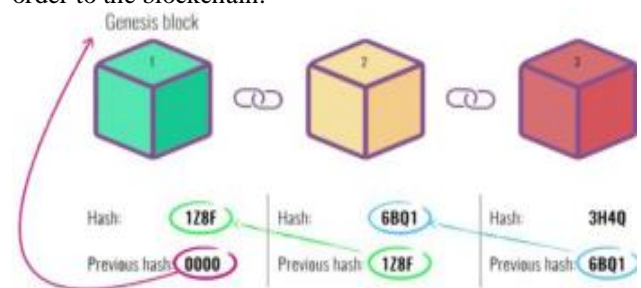


Fig.1.BlockChain Using LinkList Method.

The initial block in a blockchain is known as the 'Genesis block' or 'Block 0'. The genesis block is usually hardcoded into the software; it is special in that it doesn't contain a reference to a previous block. Once the genesis block has been initialised 'Block 1' is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root . The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header, this means to change data you would have to modify the block that records the transaction as well as all following blocks.

To make E-Voting more secure Blockchain has two more properties they are proof of work and peer to peer network

### 1. Proof of work

Proof of work is a protocol that has the main goal of deterring cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.

Proof of work is a requirement to define an expensive computer calculation, also called mining, that needs to be performed in order to create a new group of trust less transactions (the so-called block) on a distributed ledger called blockchain.

In case if we feel system is not secure some one still tampered the data we can apply proof of work property of blockchain to make system(voting) more secured and confidential. Proof of work it's a mechanism that's slows down the creation of new blocks. It takes about 10 min to calculate the required proof of work and add a new block to the chain. This mechanism makes it very hard to tampered with the block because if you try to tampered with a one block you need to recalculate the proof of work for all the blocks. So the security of blockchain come up with the its creative use of proof of work.

### 2. Peer to peer network:

Blockchain has one more property which makes them secure. A Blockchain is not stored on one person's computer. Instead, it is stored in a large network of computers called a peer-to-peer network. A computer on this network is called a node, and every node will have a copy of the Blockchain

Every a time a new block of transactions has to be added to this network, all members (nodes) of the network must check and verify if all transactions in the block are valid. If all nodes in the network are in agreement that the transactions in a block are



Fig.2. Peer-To-Peer network.

correct, then the new block will get added to every node's Blockchain. This process is called consensus.

Hence, any attacker who tries to tamper with the data on a Blockchain must tamper with the data in the majority of the computers in the peer-to-peer network. This is how Blockchains proves to be a secure method of storing data.

## III. EXISTING SYSTEM

Integrity of the election method can verify the integrity of democracy itself. Therefore the election system should be secure and strong against a range of fallacious behaviors,

ought to be clear Associate in Nursing and comprehensible that voters and candidates can settle for the results of an election. However in history, there area unit samples of elections being manipulated so as to influence their outcome. In an exceedingly electoral system, whether or not electronic or exploitation ancient paper ballots, the system ought to meet the subsequent criteria Anonymity, Tamper-resistant, Human factor.

## IV. OUR PROPOSAL

For our design we tried to create a system that doesn't entirely replace the current voting but rather integrates within a current system. We decided to do this to allow for as many different ways to vote as possible, this is so voting can be accessed by the majority of the population.

### 1. Our System:

The online voting system is an Android application through which voters can log in to the system providing their voter ID and password as for the security measure for verification in which the voter's information will be checked for matching in the database. And once the information matches or verified from the database, voter now gets the One Time Password (OTP) through their selected medium like SMS or email. The OTP will be encrypted using the play fair cipher by the same voters are not allowed.

Voters vote information privacy: One the voter makes the vote, no information related to the voter is stored in the vote database. So that no-one knew who has voted for whom.

Vote verification: Once the vote is cast, the system gives voters information of their votes successfully made in case if the vote is successful otherwise the system shows respective error or suggestion for making a vote. To use the system, initially, users need to create their account in a secure online voting system app algorithm. After all this process of verification and insertion now then to make a vote using this system, people need their valid voters can access the candidate list and then they can give their vote for the preferred ones.

### 2. Implementation model:

The proposed secure online voting system uses a MD5 hashing algorithm to make voters information safe and secure along with verification One Time Password verification (OTP) to make account accessible to genuine users only. The proposed system is an Internet-based system that requires Internet access to run. And as it is an Android-based application, the followings show the hardware and software requirements for the proposed system. For the system, end-users require an android mobile device whereas, for administration, a PC with capabilities to run light-weight server-side services and database servers is more than sufficient.

### 3. The proposed system has the following features:

**Validating Voters:** Anyone in the entire world can install this application but only those who have the valid voter's information given by the country/school/college/office for each respective election those voters are only allowed to make vote using this system. For example: to make a vote in a national election, voters need to verify by providing their valid citizenship information. In the same way ID card information is required to vote in an election of school/college/office. These following requirements are fulfilled in the system as it is most essential in the online voting system:

**Voters Privacy:** All voter information is hashed using the SHA3-512-bit hashing algorithm then only the hashed information is stored in the election database. This helps to keep the voter's information anonymous.

**Detection of Multiple vote attempts:** The system allows voters to vote only once in any election. Multiple vote attempts identification information according to their preferred election type that includes national election, school/college/office election, etc. To make the voting process more secure, the system needs voters to go through an authentication process which includes fingerprint verification or one-time password (OTP) verification send to their pre-registered phone number in the system. Figure 4 shows the overall voting process using a secure on online voting system.



Fig.3.voting process of E-voting system.



Fig.4. Generate Hash value.

## V. MD5 ALGORITHM

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding

works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264.

The main MD5 algorithm operates on a 128-bit state, divided 9. Result and discussion:

In total, blockchain algorithm will work after the voter into four 32-bit words, denoted A, B, C, and D. These are vote the candidate. Once the voter votes that vote is initialized to certain fixed constants. The main algorithm then automatically visible into the database. And its visible that which uses each 512-bit message block in turn to modify the state. The candidate got the vote, But voter identity is not revealed. And processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations displayed in the database that which candidate got the highest based on a non-linear function F, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions; a different one is used in each round:

Denote the XOR, AND, OR and NOT operations respectively[5]

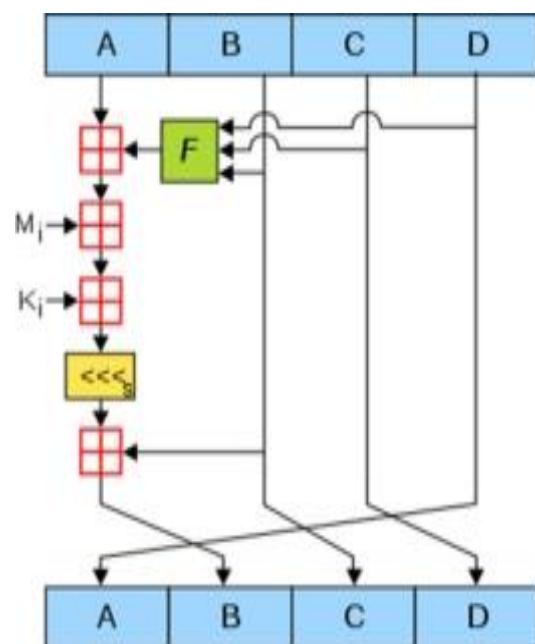


Fig.5. MD5 Algorithm.

## VI. FUTURE WORK

The system doesn't allow a user to modify their vote even if they have voted mistakenly. so in the future, a user should also be able to modify the vote and change their votes.

We also use options like eye scanner, face recognition, fingerprint recognition it provides more security.

## VII. CONCLUSION

Electors abroad are clearly a focus group that is of particular interest for those countries that are considering the introduction of e-voting in a general manner. At the same time, they are a target group that can be difficult to include in e-voting for practical reasons. Other countries see a need to introduce e-voting for their external electors but do not see the same urgency for introducing e-voting for the internal electors. However, there is no definite trend towards the introduction of remote e-voting, not even in the countries where the first steps towards it have been taken.

## VIII. ACKNOWLEDGMENT

1. We extend our sincere thanks to prof Dr.A.P.Pande.
2. We also would like to thank our project guide Assistant prof.S.S.Karve.

## IX. RESULT AND DISCUSSION

In total, blockchain algorithm will work after the voter into four 32-bit words, denoted A, B, C, and D. These are vote the candidate. Once the voter votes that vote is automatically visible into the database. And its visible that which The candidate got the vote, But voter identity is not revealed. And after all election process, The voting result is automatically displayed in the database that which candidate got the highest Vote. If someone try to change or try to tampered the data(vote) in the database. Automatically blockchain algorithm caught the tampering. And at the result site in database shows that "The data gets tampered". Then we get to know that some one try to change the vote. So because of blockchain algorithm we can give the fair decision towards election. Also some internal person whose having all voters name and id cannot take advantage of that information to vote. Because in the Application one time password system is given. voters get the OTP in their mobile after filling the respective information and then allowed to vote. So internal tampering is also not possible in the system.

## REFERENCE

- [1]. Madise, Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide

- [2]. binding Internet voting in the world.",Electronic voting, 2nd International Workshop, Bregenz, Austria,(2006) August 2-4.
- [3]. J. Gerlach and U. Grasser, "Three Case Studies from Switzerland: E-voting", Berkman Center Research Publication, (2009).
- [4]. Yi EURASIP Journal on Wireless Communications and Networking (2019) 2019:137 <https://doi.org/10.1186/s13638-019-1473-6>
- [5]. <http://aceproject.org/ace-en/topics/va/observation-of-external-voting/conclusions-of-observation-of-external-voting>. [5] <https://en.wikipedia.org/wiki/MD5>
- [6]. Y. Liu and Q. Wang, "An e-voting protocol based on blockchain." IACR Cryptology ePrint Archive, vol. 2017
- [7]. W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018, pp. 401–408.
- [8]. K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," International Journal of Electronic Government Research (IJEGR), vol. 14, no. 1, pp. 53–62, 201