Voting Solution during Covid Pandemic

Bhagyashree Shet[1], Neha B[2], Sneha Kamat[3], Sunidhi Phayde[4], Dr. Sumathi Pawar[5]
UG Students[1, 2, 3, 4] Department of Information Science and Engineering
H.O.D[5] Department of ISE
Canara Engineering College, Benjanapadavu

***Abstract* - This project is focused on Voting solution during Covid pandemic using Blockchain technique. In a democratic country like India, a single authority is responsible for maintaining huge Voting Database. If any false changes are made to it, there is no way to identify them. Also, not all people are able to come and vote at the voting booths, as they might be living far from voting center, are busy on that day, etc. This system aimed to decentralize the voting system and increase the transparency in voting. Same copies of that data will be available in different systems, so if changes are made into one of the system's data, consensus will identify by tallying them with others. Authenticated users will be able to cast vote remotely through their mobiles and desktops. Users will be sent one-time password on their devices using which they can log into the system and cast their respective votes. With the help of Blockchain, wallets of the authenticated users will be created, and in the transaction, coins will be interpreted as their vote. The user can send their respective coin (vote) from their wallet to their respective candidate wallet and these transactions will be zipped into the blocks of the distributed immutable ledger Blockchain.**

Index Terms: **BlockChain, Universal Unique Identifier (UUID), Elliptic Curve Digital Signature Algorithm (ECDSA)**

I. INTRODUCTION

This Project "Voting Solution during COVID pandemic" aims to decentralize the voting data and increase the security and transparency of the voting data. Same copies of that data will be available in different systems, so if changes are made into one of the systems data, consensus will identify by tallying them with others.

The project is a web-based application, so, authenticated users will be able to cast vote remotely through their mobiles and desktops using their credentials. Users will be asked for their credentials. Authenticated users will be sent one time password on their E-mail ids using which they can log into their system and cast their respective votes. With the help of Blockchain, wallets of the authenticated users will be created, and in the transaction, coins will be interpreted as their vote. The user can send their respective coin (vote) from their wallet to their respective candidate wallet and these transactions will be zipped into the blocks of the distributed immutable ledger Blockchain.

The voters need to enter his/her credentials for voting. The data is then encrypted and stored as a transaction. This transaction is then broadcasted to every node in network, which in turn is verified. If network approves transaction, it is stored in a block and added to the chain. Once a block is added into chain, it can't be updated or changed. Users will be able to see the results and track the voting process accordingly when needed.

The current voting system doesn't have security which is required in the modern generation, as they don't have trust in the current voting systems, there is a need to build a system that leverages security, convenience, and trust involved in voting process. Hence if voting systems use Blockchain technology to add an extra layer of security and encourage people to vote from anytime, anywhere without any hassle and makes voting process more cost-effective and time-saving.

A. Problem Statement

The aim of our project is to develop a system for “Voting Solution during COVID pandemic” using block chain technology.

This system helps to decentralize the voting data and hence, increase the transparency and security of the voting data and also, allow the registered users to cast vote remotely through their mobiles and desktops which can be used by the general public and government authorities.

II. LITERATURE SURVEY

This Literature Survey has been done to gain insights on the following divisions of our project:

1. To check whether or not the use of Blockchain technology will be useful and feasible in our application.
2. To study different existing similar applications and the drawbacks in them.

In the paper authored by Juniper Research [1], focused on usage of Blockchain in large companies. Oracle Corporation hardened security of relational databases by using more than one trusted entity for storing and updating entities. In Blockchain Technology no need of trusted parties. Instead storing and securing will be done by a group of anonymous strangers which results that Block chain technology will be very useful and feasible in our type of applications.

NYU Masters students created voting system by going through effective test cases and offered a design to show how a blockchain voting system might look like. The system, [4] Vote Watcher is most mature and tested Block chain voting implementation. Voters will be given a paper ballot after registering using current methods. The QR codes stored in ballot paper is scanned and sent to unique address of the candidate. Once the election is complete all the votes are added to the global Blockchain.

In [2] Estonian I-Voting System: An integrated circuit with 2048-bit PIN is used in ID card of elections. The signature of voter is downloaded and used for authentication. Election’s public key is used for encrypting the vote and voter’s private key is used for signing. After casting the vote it will be sent to server of vote storage which is controlled by the Estonian government.

About 280000 eligible people casted their vote using voting [3] system of New South Wales State election in 2015. The steps followed are registration with authorities, receiving of voter ID and third step is choosing a six digit PIN. Voter’s ID and PIN is used to login and cast a vote. After voting 12-digit number is received as a confirmation. The drawbacks with the Estonian model were due to raising questions on the transparency and centralization of votes that could lead to a DDOS attack.

In the paper[11] of XML encryption & XML signature, authors focused on securing the data transfer of through Web Services, but size of SOAP message data transfer is huge which bottlenecks the speed of the system.

III. METHODOLOGY

Figure 1 depicts that the voter needs to enter the Name, Email, Phone, Aadhar card number and voter Id number in order to sign in to vote. All data is then encrypted and stored as a transaction. An OTP is sent to the registered email Id and phone number, all the process needs to have a stable internet connection. When user votes to a candidate, voting information is added with block chain and sent across the network.

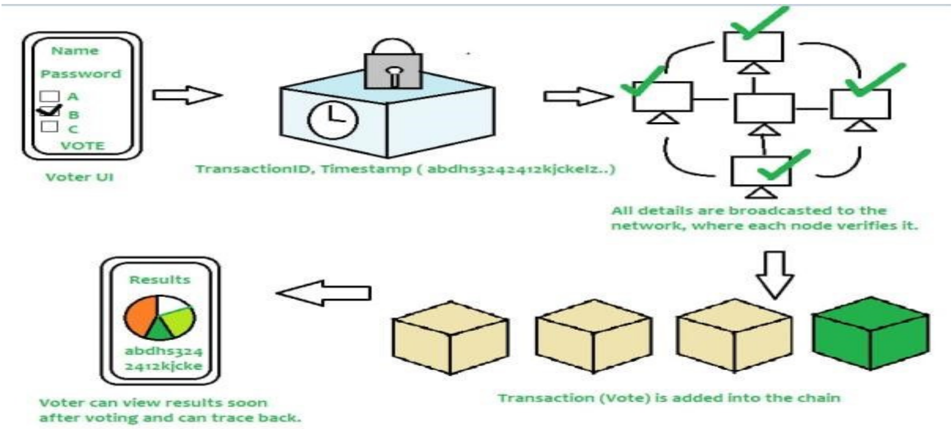

Name
Password
□ A
☑ B
□ C
VOTE
Voter UI
TransactionID, Timestamp (abdhs3242412kjckelz..)
All details are broadcasted to the network, where each node verifies it.
Results
abdhs324 2412kjcke
Voter can view results soon after voting and can trace back.
Transaction (Vote) is added into the chain

Fig 1: Block Diagram

Blockchain [5] : A blockchain is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. It is resistant to tempering of the data. It is an open and distributed ledger to record transactions between two parties efficiently and in a verifiable and permanent way. It is managed by peer-to-peer network which obeys the protocol for inter-node communication and validate new blocks. Once the data recorded, it cannot be altered. Blockchain may be considered secure as it has high fault tolerance. Decentralized consensus has therefore been claimed with a Blockchain.

OTP [6]: It is one time password which is valid for the given login session only on any digital device. They are random numbers which are used as the traditional password-based authentication. Static passwords are vulnerable to threats while OTP are not. OTP are used only for a certain logged in session and time, hence if an intruder tries to record the OTP that was already used to log in, it will not be possible as it will not be valid to perform any activities related to the OTP . And if any person have same password for almost all the system used by him/her then they are more vulnerable to the attack, while OTP authentication is a very safe method to use.

Secure Hash Algorithm 3 (SHA-3) [7]: SHA-3 is recently added to secure hash algorithm standards. It uses mathematical algorithm to map data of any size (message) to a fixed size bit string (hash). It uses Keccak algorithm which is based on un-keyed permutations as opposed to other usual hash functions' constructions.

Keccak algorithm [8]: A new approach called sponge and squeeze construction is used in Keccak, which is a random permutation model. The variant used in this project is SHA-3 with 256-bit of output (SHA3256).

Universally Unique Identifier (UUID) [9]: It is a 128-bit number used to identify information in computer systems and are unique. The probability of the similarities between two UUID is 0 or <1 which is negligible. It can be created by anyone of us and use it to identify something. They are later combined into one database and transmitted on the same channel.

Elliptic Curve Digital Signature Algorithm (ECDSA) [10]: It is a cryptographic algorithm which is used to ensure that votes are spent by the rightful. Following are the concepts of ECDSA:

- Private Key: A secretly randomly generated single unsigned (32 bytes) number key by a person.
- Public Key: A 65 byte number which is not secretly generated and calculated by private key. It is mainly used to check if the digital signature key is legit or not.

- Signature: A mathematically generated hash with 71 – 73 bytes long. It is used along with public key and produced from hash and private key

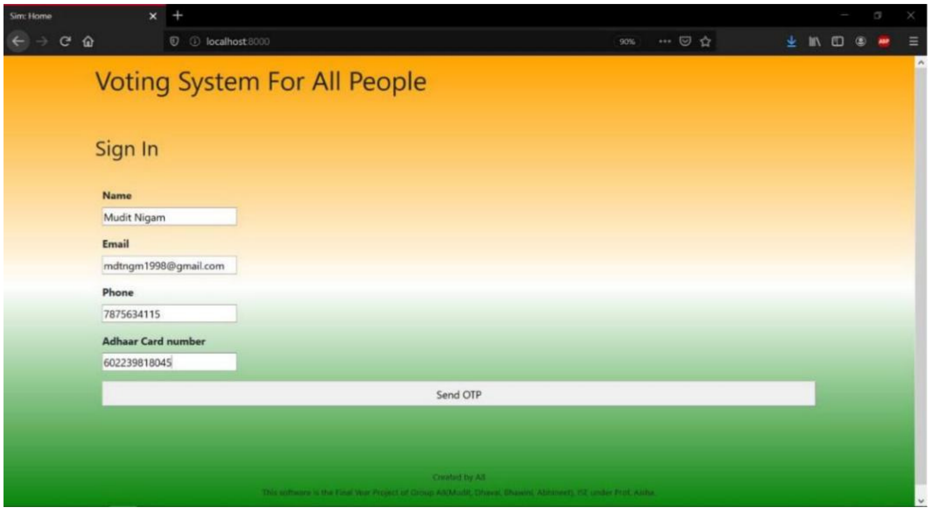
- Remote Login: A login system will allow a user terminal to connect to a host computer via a network to interact with host.

IV. IMPLEMENTATION AND RESULT

HTML, CSS and JavaScript is employed as front end which is used to craft the user interface. SQLite, Django and Python is employed as back end. The system developed is user-friendly and can be used by any user without any prior explanation. This is a user friendly system where only limited resources like laptop or mobile and internet connection is required to caste vote in this Covid pandemic. The system is well developed for naïve person to vote, we can also save time and cost from this system. It is secured system for remote voting.

The Login Page:

The home page of the application consists of the login page. In this page user has to provide his/her various details consisting of Name, Email-ID, phone number and Aadhaar card number. After providing the necessary details, the user presses the Send OTP button for the verification and authentication purposes.



Voting System For All People

Sign In

Name
Mudit Nigam

Email
mdtngm1998@gmail.com

Phone
7875634115

Adhaar Card number
602239818045

Send OTP

Created by A8
This software is the Final Year Project of Group A8(Mudit, Dhaval, Bhavini, Abhineet), ISE under Prof. Aisha.

Fig 2: Login Access

If OTP is correct the voter can proceed in voting else an error message is displayed. Blockchain also get verified by broadcasting the transaction to every node in network. If network approves transaction, it is stored in a block and added to chain. Once a block is added into chain, it stays there forever and can't be updated. Users will now have to vote from the list of eligible candidates and copy paste the private key which was sent along with OTP from their email or phone number and see results and also trace back transaction if they want individually.

V. ANALYSIS

Comparing the existing systems and the methods used, advantages and limitations are listed below in the tabular form. The methodology/algorithm used in the proposed system is more efficient, compared to the existing system.

Table 1. Analysis Table

Name of the Paper	Methodology/ Algorithm	Limitations	Advantages
[1] Juniper Research paper	Hardening security of relational databases using many entities.	The system was handed over to one or two entities, hence it was most likely to be hacked.	Blockchain remove the need for a trusted authority.
[2]. i-Vote system	Registering with authorities and receiving a voter ID and choosing a 6 digit number for casting vote.	Estonian model raised questions on centralization of votes that could lead to a DDOS attack.	The voter can view the blocks after he finishes voting hence maintaining in transparency.
[3]. Vote book –Created by NYU Masters students	Usage of block chain for booking vote	The blocks are not visible to the voters.	Here the blocks are visible to users making the voting system more transparent.
[4]. Vote Watcher	Vote Watcher uses Block chain and uses an external source to create node and add all the data at the end.	Uses an external source, an offline and online mode for creating Block chain.	It is completely dependent on online.

VI. CONCLUSION

We have implemented an online voting system which lets a voter vote from a remote location. With the help of Blockchain we have decentralized the database. Decentralized database will increase the security and transparency of the data and never allow anyone to make fraudulent changes to by having the same copies of that data available in different systems, so if changes are made into one of the systems' data, consensus will identify by tallying them with others. To increase the security of the system authenticated users will be sent a one-time password on their respective devices using which they can log into their system and cast their respective votes.

REFERENCES

[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

[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

[3] 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 E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007

[4] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40- 46, May 2008

[5] A. E Keshk, “Development of remotely secure E-voting”, 5th International Conference on Information and Communications Technology, pp. 235.

[6] Wikipedia Contributors, ‘One-time password’, April 19 2021 [Online]. Available : http:// One-time password - Wikipedia

[7] Guest Writer, ’Blockchain Technology Explained (with Infographic)’, Jan 2 2021. [Online]. Available: http:// Blockchain Technology Explained (With Infographic) - Tech4Fresher.

[8] Wikipedia Contributors, ‘SHA-3’, April 13 2021 [Online]. Available : http:// en.wikipedia.org/wiki/SHA-3

[9] Wikipedia Contributors, ‘Elliptic Curve Digital Signature Algorithm’, April 6 2021. [Online]. Available: http:// Elliptic Curve Digital Signature Algorithm - Wikipedia

[10] Wikipedia Contributors, ‘Universally unique identifier’, April 22 2021. [Online] .Available: http:// Universally unique identifier - Wikipedia

[11] S Pawar, NN Chiplunkar, Open source APIs for processing the XML result of web services, 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI-2017), MIT, Manipal, pp 1848-1854.