



Blockchain Based Voting System

Charan Reddy¹, K Sriraj², C Gangadhar³, P Swarnalatha⁴

¹ Vellore Institute of Technology, India, vundelacharan@gmail.com

² Vellore Institute of Technology, India, srirajreddy42749@gmail.com

³ Vellore Institute of Technology, India, gangadhar.reddy2018@vitstudent.ac.in

⁴ Vellore Institute of Technology, India, swarnaa2k2@gmail.com

ABSTRACT

The Voting/Electoral system is that the backbone of Each and Every Country and Organization. The main goal of voting (in a scenario where the citizens have a right to vote) is to come up with their leader of their choice. At Present there are various voting is conducted in various methods such as Ballot Voting, E-Voting also known as Electronic Voting System, Missed Call Voting. Various problems are during Election Period as some of them include ridging votes/fake votes during election, insecure or inaccessible polling stations, inadequate materials and also inexperienced personnel. To overcome this problems we have used Blockchain Technology to make Unique ID's for each vote.

In this paper, we have tried to sort out issues faced by various voting systems. And make Voting more Secure by using various authentications.

Key words : Anonimity, Authentication, Blockchain, Voting, Qr code.

1. INTRODUCTION

Election is extremely crucial and very serious event in any democratic country. the foremost common way during election is Fake votes thru paper based system, but is it not time to bring voting into the 21st century of recent technology? Digital voting is that the use of electronic devices, like voting machines or an online browser, to cast votes. These are sometimes mentioned as e-voting when voting employing a machine during a polling place and voting when employing a browser. Security of digital voting is usually the most important concern when considering to implement a digital voting system. With such monumental decisions at stake, there are often little question about the system's ability to secure data and defend against potential attacks. a method the safety issues can be potentially solved is thru the technology of blockchains.

Blockchain technology originates from the underlying architectural design of the cryptocurrency bitcoin. It's a sort of distributed database where records take the shape of transactions, a block is a collection of those transactions. With the utilization of blockchain a secure and robust system for Election will lead to Secure voting. This report outlines our idea of how blockchain technology could be next game changer with more secure system.

Also with Blockchain Technology, We will adding the more types of security Authentications Which helps to make Voting more Secure. Three Authentications are such as Face Authentication, Qr code Validation, The last one Otp verification. We also added the Manual Authentication in Which Admin/polling staff has to verify the voter Before Voting. Voting Can be done after the Manual authentication only. If Admin not verify the person He cannot vote. Now I'll be discussing about our security Authentications.

OTP verification

At the Time of Registration User will be asking to Provide a Email Id. While the Voter Attempted to Vote. Then OTP will be sent to the Mail id. The voter needs to Enter the OTP to proceed to Next step. We Have used Node mailer For doing The OTP verification

Face Authentication

At the Time of Registration User will be asking to Capture a photo of user Which will be stored In our database. We will be verifying the Face During Voting. We have used Microsoft Azure API to Verify the Voter.

QR Code validation

After The Successful Registration, Voter will be provided a QR code which contains Unique Id. That will be validated While Voting After the Face Authentication. We will be asking the user to upload the QR code. After the successful validation only User is allowed to Vote.

After this Three Successful Authentications only the user will be allowed to vote.

3. LITERATURE SURVEY

It Concentrates on survey and analysis of different Type of voting systems.

In this system, the voter can cast the vote by sending SMS to the system using any kind of hand set through the mobile switching center. The voter has to first dial a tollfree number in which he has to answer through SMS depending upon the questions asked on recorded call.[1]

In this system, the user can create their own voting ballot. The system would be like that the user won't have to register any account, they just have to provide the Aadhaar Card number. The local admin i.e. the user who creates the voting ballot will be given a unique serial code by our system which the local admin broadcast to all the user's who are going to vote.[2]

One of the distinctive highlights of blockchain-based Distributed Autonomous Organizations (DAO) is that the lack of a focal authority. Changes to blockchain information are accomplished through agreement among blockchain network members, as opposed to through a focal hub's legitimate choice. Additionally, administration, i.e., changes to highlights and hidden ASCII archive, is accomplished through a decentralized system. As reception of blockchain has expanded, the need to develop and receive new highlights has developed. These progressions feature the system by which the organization, as opposed to a focal hub, decides. One change, in specific, proposed increments to the square size to influence adaptability limits, has been especially steady the administration components utilized by divergent blockchains.[3]

As innovation progresses, numerous nations have now settled on electronic democratic frameworks. Any democratic framework should follow standards of straight forwardness and fair-mindedness to accomplish reasonableness; the electronic democratic cycle should likewise be ensured against

digital assaults or forswearing of-administration assaults (DDOS) on the grounds that such assaults may influence the handling time in casting a ballot methods and indeed, even impede the reasonableness in casting a ballot. This examination sets up an organization security component for casting a ballot frameworks dependent on blockchain innovation. The blockchain component utilizes a circulated engineering that can forestall framework closure coming about because of malignant digital assaults; also, any client in the blockchain can confirm information uprightness, which fulfills necessities of straightforwardness and unprejudiced nature in casting a ballot frameworks.[4]

E-casting a ballot, then again, is another moving, yet basic, theme identified with the online administrations. The blockchain with shrewd contracts arises as a decent possibility to utilize in improvements of more secure, less expensive, safer, more straightforward, and simpler to-utilize evoting frameworks. Ethereum and its organization are quite possibly the most reasonable ones, because of its consistency, far and wide use, and arrangement of brilliant agreements rationale. An e-casting a ballot framework should be secure, as it ought not permit copied casts a ballot and be completely straightforward while ensuring the protection of the participants.[5]

Bitcoin presents a progressive decentralized agreement component. Be that as it may, Bitcoin-determined agreement components applied to public blockchain are insufficient for the organization situations of maturing consortium blockchain. We propose another agreement calculation, Proof of Vote (POV). The agreement is composed by the disseminated hubs constrained by consortium accomplices which will go to a decentralized discretion by casting a ballot. The key thought is to set up various security personality for network members so the accommodation and confirmation of the squares are chosen by the organizations' democratic in the group without the contingent upon an outsider middle person or wild open mindfulness. Contrasted and the completely decentralized agreement Verification of Work (POW), POV has controllable security, assembly unwavering quality, just one square affirmation to accomplish the exchange certainty, and low-postpone exchange check time.[6]

Progressively advanced innovation in the present aided numerous individuals lives. In contrast to the constituent framework, there are numerous regular employments of paper in its execution. The part of safety and straightforwardness is a danger from a still far reaching political decision with the ordinary framework (disconnected). General decisions actually utilize a brought together framework, there is one association that oversees it. A portion of the issues that can happen in conventional constituent frameworks are with an association that has full command over the dataset and framework, it is feasible to mess with the data set of significant freedoms. Blockchain innovation is one of the solutions, because it accepts a decentralized framework and the whole information base are claimed by numerous clients. Blockchain itself has been utilized in the Bitcoin framework known as the decentralized Bank framework. By embracing blockchain in the conveyance of information bases on e-casting a ballot frameworks can diminish one of the conning wellsprings of data set control.[7]

The above proposed systems do not identify its users with the simplicity and compatibility of the its process as the majority being ill-educated. The systems are complex and require

explicit tutoring and monitoring for efficient working of the system. Therefore, we provide a suitable software which satisfies all the fundamentals requirements with minimal overhead cost.

4. METHODOLOGY

The development of the application is divided into four basic modules for which a brief

- Database Design**
- Voter Registration**
- Voting Authentication**
- Voting/Vote Count**

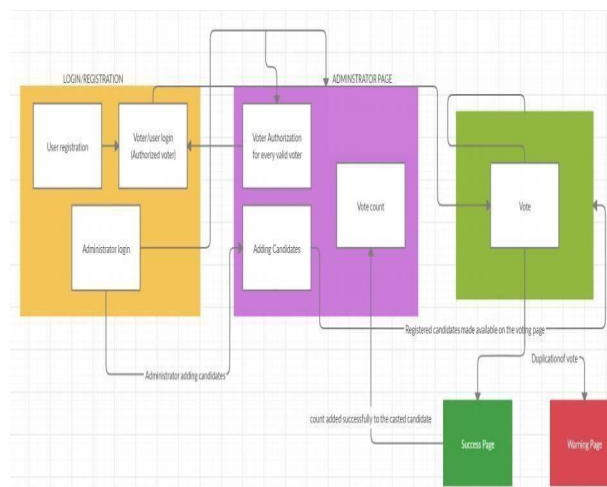


Fig1

Figure 1 shows architectural diagram of Blockchain Based voting system

4.1 Database Design

The module describes the database structure and design which uses two structured schemas or here collections admin schema and user schema. Admin schema describes the document related to candidate details and vote count for that candidate handled by the administrator. User schema describes the document related to the user/voter details which is incorporated by the registering through a register form and validating ever user by the administrator.

4.2 Voter Registration

The module describes the backend mechanism of registration and login in node.js using npm package passport.js. The user registers itself filling in the details provided in the form and logs in with the username provided by the administrator. Administrator login is defined explicitly

as there exist a single handler to administrator page. After registration of a new voter, Administrator verifies the authenticity of the voter from his panel.

4.3 Voting Authentication

First the voter should enter the OTP sent to their Email id, after verification, Voter uploads a Qr code, which represents the voter id and then Face authentication is done finally to verify the voter. Microsoft Azure is used for Face authentication when we used a Machine learning model to match the face already saved in database during registration and captured face during verification.

Blockchain is used to create a unique decentralised transactions for each voting session. We will have log of transactions performed.

4.4 Voting/Vote Count

This module describes the voting logic and the counting of the votes for every candidate standing in the election. Only the authorized user will be allowed to use the voting portal. The voting option for candidates will redirect through the success page if the voter has voted once. Else, he will be redirected to the warning page which shows the rejection of the casted vote.

5. CONCLUSION

Voting percentage can be improved as now giving votes is very easy. Voters can give vote from their place of convenience without any problem. It will be very convenient for voters to do voting now. Booth capturing was always a issue during election and sometimes voters are threaten to vote for a particular candidate. It will not be a issue now. Lot of violence is done during elections to threaten people, which can be reduced. Conducting voting involves lot of money and security. But by now using online Blockchain voting system, Spending money and as a result we can Decrease the False Voting Percentage

6. FUTURE ENHANCEMENT

This Blockchain Based Voting System Application can be made even more secure by using more biometrics such as Fingerprinting , Cornea Detection etc. The Face Authentication is here based on Machine learning model in Microsoft Azure, Instead there should be a tamper proof model developed for this Authentication purpose with good hardware. So it helps to increase the security of the system. Other methods Which can be used are “cornea detection” and “biometrics”. But the problem is that it decreases the scope of the platform because these need more electronic components like fingerprint scanner to implement. So, it will decrease the flexibility to cast the votes at their convenience. But if these are implemented their will be no space for fake voting.

REFERENCES

1. MD Shamsur Rahim, Ehtesham Chowdhury **Analysing Online Voting Systems for Flaw Detection**
2. Dr. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair **International Conference on Innovations in Information, Embedded and Communication Systems(ICIECS)**
3. Stephen DiRose; Dr Mo Mansouri. **Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations**
4. Hsin-Te Wu; Chang-Yi Yang **A Blockchain-Based Network Security Mechanism for Voting Systems**
5. Ali Kaan Koc; Emre Yavuz; Umut Can Cabuk; Gokhan Dalkilic **Towards Secure E-voting Using Ethereum Blockchain**
6. Kejiao Li; Hui Li; Hanxu Hou; Kedan Li; Yongle Chen **Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain**
7. Rifa Hanifatunnisa; Budi Rahardjo **Blockchain Based E-Voting Recording System Design**
8. Tadayoshi Kohno, Adam Stubblefield, AvieRubin, Dan S. Wallach, “**Analysis of an Electronic Voting System**”, Johns Hopkins University Information Security Institute TechnicalReport, TR2003-19, July 23,2003.
9. Pankaj Kumar Malviya “**E-VOTING SYSTEM USING CLOUD IN INDIAN SCENARIO**”, Department of Software Engineering, IIIT Allahabad,Uttar Pradesh, India.
10. HimanshuAgarwal, G.N.Pandey, “**Online Voting System for IndiaBased on AADHAAR ID**”, Dept. of Software Engineering Indian Institute of Information Technology, Allahabad-211012, India.
11. 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
12. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: **End-to-end voter-verifiable optical- scan voting**, IEEE Security Privacy, vol. 6, no. 3, pp. 40- 46, May 2008.
13. Chaum, D. (2004) **Secret-ballot receipts: True voter-verifiable elections**, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.
14. Hao, F., Ryan, P. Y. A., and Zielinski, P. (2010) **Anonymous voting by two-round public discussion**, IET Information Security, vol. 4, no. 2, pp. 62-67, June 2010.
15. Aishwarya Indapwar, Manoj Chandak,Amit Jain **E-Voting system using Blockchain technology**, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9, No.3, May - June 2020