

TOWARDS SECURE E-VOTING USING ETHEREUM DAPP

Gaurav Pachbhai
Department of Information
Technology
Karmaveer Dadasaheb
Kannamwar

Ankit Dhote
Department of Information
Technology
Karmaveer Dadasaheb Kannamwar
College of Engineering

Pratik Mendhe
Department of Information Technology
Karmaveer Dadasaheb Kannamwar
College of Engineering
Nagpur, Maharashtra, India

Kamakshree sharma
Department of Information Technology
Karmaveer Dadasaheb Kannamwar
College of Engineering
Nagpur, Maharashtra, India

Rajeshwari Jambhe
Department of Information Technology
Karmaveer Dadasaheb Kannamwar
College of Engineering
Nagpur, Maharashtra, India

Project Guide-Prof. Harish Gorewar
Department of Information Technology
Karmaveer Dadasaheb Kannamwar
College of Engineering
Nagpur, Maharashtra, India
harishgorewar.it@kdkce.gmail.in

Abstract — Voting is a crucial component of a nation's governance. Voting is still done by physically visiting to polling places. Security is not guaranteed by this procedure, and instances of tampering have been noted. With the help of Blockchain technology and an online voting system, this study seeks to eliminate these problems with the voting process. Every vote is secure thanks to blockchain technology and hashing. One choice is regarded as a transaction in this instance. A private blockchain that incorporates election events into this distributed ledger is developed using a peer-to-peer network. The design of the programme obscures the user from the intricate details of the underlying architecture. Each voter is tracked using their government-issued Aadhar ID. This number is used by the plan to guarantee that each voter only has one opportunity to cast a ballot. All peers are in sync when the decision is shown as a transaction. The votes are encrypted, hashed, and added to the blockchain to improve security and create a chain of blocks because each peer is associated with a public and private key. Using a vote is not a ballot cannot be used to determine the voter. In this study, a peer-to-peer network is created with a minimum of three peers. Because voting takes place online, it is expected that this paper will increase voter turnout. How scalable a blockchain programme can be is determined by the secondary memory limit of the peer.

Keywords— Blockchain, Ethereum, Git, p2p, smart contract, solidity, truffle, sublime text, Ganache, truffle pet-shop

I. INTRODUCTION

The right of the people to select their leaders is referred to as democracy. In order for people to choose their

government leader, voting is a crucial step. A democratic, independent, and unbiased electoral system is required. Since everyone must be able to freely express their opinions, it must be a transparent and secure process (Bosri et al., 2019).

A large portion of the global populace has lost faith in the electoral process (Inzamam-Ul, YYYY). A lot of mediators are in charge of and monitor the Conventional voting (Asraful and Rashid, 2018). The various ways that individuals define "blockchain innovation" can be confusing. They discuss different virtual currency systems occasionally, the Bitcoin Blockchain occasionally, and smart contracts occasionally. They are referring to dispersed records, or a list of transactions that is not centralised but instead kept on numerous PCs rather than a single server. They are referring to dispersed records, or a list of transactions that is not centralised but instead kept on numerous PCs rather than a single server. Blockchain technology has been around since the 1980s. Nevertheless, bitcoin is the reason it is presently getting more attention. Despite having no inherent worth and no centralised authority to regulate transactions, bitcoin has been hailed as the first illustration of a digital asset (digital currency) that can be used for financial transactions since its creation in 2009 [1]. The fact that blockchain Equations served as the underlying technology for its development is also important. The electoral procedure is essential in a democracy. Due to widespread criticism of the government and foreign meddling in domestic affairs, the freedom to vote is now more important than it has ever been.

II. LITERATURE SURVEY

A. Online Voting System For India Based on AADHAR ID - Himanshu Agarwal, G. N. Pandey in the year 2013 [2]

Before a vote is recorded in the primary database, a high security password must be verified, and a fingerprint authentication module is used. The voter can check to see if their ballot was given to the right person or group. Manual tallying of the votes is an option, but this system immediately counts the votes, guaranteeing that every vote is taken into account and that none will be misinterpreted.

B. Biometric voting system using aadhar card in india - S Chakraborty, S Mukherjee in the year 2016 [3]

In order to create a secure voting machine with a distinctive mark as the Aadhar card database is used, an electronic voting machine using fingerprint technology has been developed. However, it includes the same threats as any other EVM, including threats to the physical security of the machines, safe voting data storage, and vulnerable software.

C. Trustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit Shahzad Raju, Jon Crowcroft in the year 2019 [4]

A framework is proposed that makes use of efficient hashing methods to guarantee data protection. The idea of block creation and block sealing is presented in this paper. Blockchain can be adjusted to satisfy polling process requirements thanks to the block sealing concept.

D. Security Analysis of India's Voting Machine - Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri in the year 2010 [5]

Real Indian EVMs were used for the security analysis.

According to this study, there are numerous methods to tamper with an electronic voting machine (EVM), including changing the machine's state, replacing the CPU and/or unit with a look-alike, and installing unauthorised software. The suggested voting system has no significant hardware requirements, eliminating all of the aforementioned EVM drawbacks. Additionally, the suggested model makes use of blockchain to guarantee that it is simple and secure to transfer votes to candidates' ballots.

III. EXPERIMENTATION DETAILS AND PROPOSED FEATURES

Several research projects on employing better It is a private blockchain for software development using Corda and Ethereum right away. used to set up a personal Ethereum blockchain that resembles the real global blockchain and allows you to run tests, execute orders, and try out the United States of America while still having control over how the blockchain operates. It comes with flavours like election-improvement technologies. These studies discuss a variety of dangers associated with implementing electronic voting systems, including software difficulties, dishonest volunteers, network capacity issues, and hacker difficulties. We've suggested integrating the Ethereum Blockchain technology into the design of the current electronic voting system. Comparing the proposed system to the current one, the following benefits are present:

- Users will have unique ids so double voting is not possible.

- Because the voting transactions are stored on the Ethereum Blockchain, which is immutable, they cannot be altered.

The voting logic will be contained in a smart-contract that is developed in the Solidity programming language in the proposed system. Once created, smart contracts are compiled using truffle to produce ab and byte code. It is impossible to make changes to a contract once it has been created and distributed on the blockchain. The variables and methods in the built contract can be accessible via web3.js, which also allows interaction with the smart-contract.

Candidates who will be running for office can be added using the admin login. The registration method will allow voters to register themselves on the portal. Only users with valid credentials will be allowed to cast ballots in the election after admin has verified the information provided by registered users.

IV. FUTURE WORK

Generating data and reports based on various factors, such as sex, geography, age, and so forth. The administration tasks that are organised with the Aadhaar framework using Aadhaar APIs will depend more on other future developments. We believe that secure technology will be used by electors to make their choice. The voter's device may already contain malicious software, which enables programmers to change or alter a decision even though our system is secure. The inability to alter a vote in the event of a client error is one of the drawbacks of our system. The customer will only have the opportunity to choose once. As a result, we might want to start making progress.

V. CONCLUSION

Applying a web-based voting solution can improve and secure the current voting process. A voting method that is both more accessible and safe might use blockchain technology. Voters can easily login and exercise their right to vote using the planned blockchain-based e-voting system, which controls the election process. We think voting systems based on blockchain will eventually take the place of traditional voting methods. Prior to the invention of blockchain, electronic voting procedures were unsatisfactory since they were neither easily auditable nor sufficiently simple for both organisers and voters. Additionally, they demand a pricey setup with a lot of work. A free, secure electronic voting process can be arranged by any group using the Ethereum blockchain. Groups, affiliations, or registered corporations should initially consider using this invention for board decisions, general meetings, or investor or member voting. A coordinated effort from the coordinators in mining activities or some involvement with excavators may be necessary for scaling up to the national level. The proposed framework, which incorporates the following, provides a helpful contrast to the existing, restrictive electronic voting frameworks. It does not address all of the issues related to electronic voting.

1. Free, open-source, and peer-reviewed software
2. Commonplace
3. Reliable
4. Permitting free, independent evaluations of the results,

This addresses the verification of security criteria such as voting app transparency, integrity, and non-repudiation, but it didn't handle the identification of participants using a reliable method, such as a biometric attribute. Ethereum and smart contracts are innovative additions to the blockchain that prevent it from being limited to the perception of a digital currency (coin) and turn it into a flexible answer for a number of internet-related problems in the modern world. These developments might pave the way for blockchain acceptance.

VI ACKNOWLEDGMENT

We appreciate the guidance and assistance provided by our mentor Prof. H. V. Gorewar and the department head Prof. Sunanda Khandiat mam. We also like to express our gratitude to the anonymous reviewers who offered insightful comments on our project script.

VII. REFERENCES

- [1] https://www.researchgate.net/publication/329396804_Online_Voting_Application_Using_Ethereum_Blockchain
- [2] Himanshu Agarwal and GN Pandey. Online voting system for india based on aadhaar id. In 2013 Eleventh International Conference on ICT and Knowledge Engineering, pages 1–4. IEEE, 2013.
- [3] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. International journal of Innovative research in Computer and Communication Engineering, 4(4), 2016.
- [4] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7:24477–24488, 2019.
- [5] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of india's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security, pages 1–14, 2010.
- [6] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.