BLOCKCHAIN ENABLED DECENTRALIZED TRUST MANAGEMENT AND SECURE VOTING SYSTEM

Mrs. P. DEEPA
Associate Professor
Computer Science Engineering
Panimalar Engineering College
Chennai, India

GUNA M
Student
Computer Science Engineering
Panimalar Engineering College
Chennai, India

GODSON RAJ R
Student
Computer Science Engineering
Panimalar Engineering College
Chennai, India.

BADHRI KESAVA RAJA S M
UG Scholar
Computer Science Engineering
Panimalar Engineering College
Chennai, India.

***Abstract*— It has always been contentious and subject to varying voter perceptions how voting events turn out in centralized settings. Most today's electronic voting systems are based on centralized servers, where participants must have confidence in the integrity of the process to produce accurate results. Using blockchain technology, we propose a novel approach in this paper for a decentralized platform for trustless voting that addresses trust issues. One vote per mobile phone number for each poll with privacy assurance and the guarantee of data transparency and integrity are the main features of this system. The voting rules will be implemented for each voting event by the organizer's using transparent, trustworthy, and deterministic smart contracts on top of the Ethereum Virtual Machine (EVM), which acts as the Blockchain runtime environment. Users' mobile phone numbers can be used to verify them without the aid of a third-party server. The system is functional, according to the results, and could be the first step towards creating settings that are ideal for such experiences.**

Keywords—Voting, Blockchain, Ethereum, Authentication, EVM, Smart Contract, trustless, decentralized, MSISDN

I. INTRODUCTION

Voting has consistently been recognized over time as the main way that people express their opinions on contentious issues and debates. It allows individuals to formally express their preference regarding a ballot question, candidate election, political party, and other issues. Unfortunately, voting is heavily reliant on the confidence imposed by the running of the election's organizing authorities. Several allegations criticizing the election processes have surfaced over the years. This architecture, in which data and the application's business logic are stored on government servers, is used by most developed E-voting solutions. Thistopology has significant disadvantages in some applications despite appearing practical in others:

1) Inadequate data integrity and security precautions.
2) A solitary weak point.
3) A lack of centralized control and secure transaction validation protocols.
4) A puzzling runtime option.
5) The server is running unidentified business rules.

The blockchain, on the other hand, is a relatively new technology that guarantees data immutability through cryptographic operations, consensus algorithms, and protocols while providing network decentralization without a single point of failure. Deploying decentralized applications (DApps) on the Ethereum Blockchain, an open-source distributed computing platform with a Turing-complete scripting language, allows software developers to take advantage of the distribution property inherited from Blockchain technology. Therefore, the following blockchain features will be present in DApps:

Decentralized validation and control via consensus procedures.

1) Runtime environment that is transparent.

2) Run-time environments for public business rules.

3) High-availability.

Even in the telecommunications sector, blockchain is becoming more popular.

In this paper, we propose an online voting platform that is decentralized and based on Blockchain technology, with the goal of addressing the trust issues that are associated with traditional E-voting systems. This system introduces a cutting-edge method for verifying and authenticating the voters who are eligible to vote.

This solution's main advantages include: (1) Enforcing voting data immutability and data integrity; (2) Assuring voting system reliability and dependability; (3) Decentralizing voter registration and validation mechanisms; (4) Transparency, clarity, and determinism of the voting environment; (5) Public visualization of the smart contracts votes; and (6) Limiting each voter to one vote per legitimate Mobile Station International Subscriber Direct.

II. LITERATURE REVIEW

In this section, we present a number of solutions that make an effort to combine blockchain technology and electronic voting in order to enable decentralized voting. The added benefits of our suggested system over the alternatives are then highlighted

a) In their article titled "Towards Secure E-Voting Using Ethereum Blockchain," Ali Kaan Ko and colleagues discuss a decentralized voting system built on the Ethereum Blockchain. It states that in order to be secure, an electronic voting system must be completely transparent (privacy-aware) and not permit duplicate votes. It is advised that the E-Voting application be turned into a smart contract, and users with active EOAs be given the ability to vote on that contract. However, since the EOAs receive their right to vote from a Centralized Authority in order to become eligible voters, this solution lacks a genuine automated address verification protocol. Transparency of business rules and a single vote restriction per EOA are its main benefits.

b) The Future of E-Voting: Tarasov et al. covered the topic of electronic voting and its potential application to blockchain technology in their paper titled "The Future of E-Voting." In addition to the inherent qualities of Blockchain DApps, such as transparency, privacy, and integrity, this solution suggests a registration phase to confirm users' identities. The protocol's first step, registration, is necessary for identity verification for audit purposes. It facilitates tracking which voters have cast ballots. Despite using the Challenge-Response handshake protocol, the verification process still requires a server (Centralized Authority) to handle it and add the users' data (email addresses) to the database. It is important to note that email addresses are currently simple to forge.

c) Voting that is decentralized, open, and trustworthy on the Ethereum blockchain: In his paper titled "Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain," Fernando Lobato Meeser discusses two different types of persistent problems with e-voting solutions. First, since the results of the smart contract can be tallied by anyone before all the votes have been cast, and second, because the recorded votes can be linked to public keys, voting is anonymous. The author of this paper describes the implementation of a voting system as an Ethereum smart contract that makes use of threshold keys and linkable ring signatures. However, this approach once more involves a registration phase, and voters depend on a Centralized Authority to register their public key in order to cast a ballot.

d) Taking Trusted Tallying Authorities Out of Self-Enforcing E-Voting on Ethereum Patrick McCorry et al. claim in a published paper that their protocols preserve voter privacy while enabling anyone, including observers, to independently confirm the validity of the election without relying on the government. They do this by using the Direct Recording Electronic with Integrity (DRE-i), Open Vote Network (OV-net), and DRE-i with Enhanced Privacy. However, before the elections begin, their system needs a governing body to set up a list of registered voters and transfer it to the Ethereum Blockchain. For some uses, having a predefined list of voters is a good option, but fully decentralizing the voting process is still difficult.

.

III. RELATED WORK

The ability of blockchain technology to offer secure and decentralized systems has attracted a lot of attention. Significant research has been done in recent years to create secure voting systems and blockchain-based trust management. We review some of the relevant works in this section.

The idea of a blockchain-based voting system put forth by Nakamoto in the Bitcoin whitepaper in 2008 is one of the earliest works in this field. Since then, a number of researchers have suggested various blockchain-based voting systems. For example, Chen et alwork .'s from 2018 proposed a blockchain-based voting system that makes use of smart contracts to guarantee privacy, security, and transparency. Similar to this, Roohi et alwork .'s from 2020 suggested a decentralized voting system that makes use of blockchain technology to thwart voter fraud and maintain transparency.3.2. Detection of hand landmarks using MediaPipe

Another area where blockchain technology has been heavily utilized is trust management. A blockchain-based trust management system that uses reputation scores to gauge user trustworthiness was proposed by Noyan et al. in their work from 2020. Similar to this, Khan et al work .'s from 2021 proposed a decentralized trust management system thatmakes use of blockchain technology to store trust data and offer a secure and transparent platform for trust assessment.

There has been research into using blockchain technology for secure data sharing, in addition to voting and trust management. In their 2018 research, Li et al. proposed a blockchain-based system for efficient and secure data sharing. Similar to this, Yang et al work.'s from 2019 suggested a blockchain-based data sharing platform that guarantees data security and privacy. The coordinates in the.csv file was collected and then sent via a panda’s library method to identify null values.

Overall, the use of blockchain technology for decentralized trust management and secure voting systems has gained significant attention in recent years. While there are still challenges to be addressed, such as scalability and interoperability, blockchain technology has shown promise in providing secure and transparent systems for various applications.

IV. PROPOSED SYSTEM

We introduce our suggested voting system in this section, which aims to remove the obstacles that currently exist in blockchain-based electronic voting systems. Fig. 1 depicts the proposed system architecture and the interactions of the system’s parts at a high level.

A. System Components

The following elements make up the suggested platform:

Web application: Event administrators can create and manage new voting events with the help of the web application

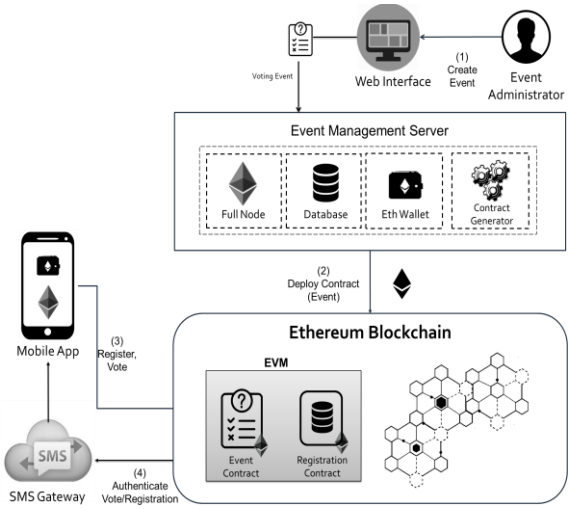

Fig. 1. System Architecture

Every voting event is represented as a unique Smart Contract on the Blockchain network. Before sending an HTTP request containing the entered data to the event management server, the administrator completes the questions and their corresponding answers. The purpose of this Web application is to provide an Application Programming Interface (API) that can be used by any user to create new voting events.

Using blockchain technology, we want to create a secure voting system and decentralized trust management system that guarantees privacy, security, and transparency. Blockchain technology will be used in the proposed system to create a tamper-proof and immutable ledger for recording votes and maintaining trust data.

The trustworthiness of users will be assessed by the trust management system using reputation scores. The blockchain will be used to store the users' reputation scores, making them public and open to all. This system will guard against the tampering of trust data and offer a safe environment for trust assessment.

The voting process will be set up to guard against voter fraud and maintain election integrity. Votes will be cast anonymously, securely, and accurately thanks to a system that combines blockchain technology with cryptographic methods. As a result of the votes being recorded on the blockchain, the election will have a transparent and verifiable record.

To ensure the scalability and efficacy of the proposed system, we will use a hybrid consensus mechanism that combines Proof of Work (PoW) and Proof of Stake (PoS) algorithms. A balance between security, scalability, and energy efficiency will be offered by this hybrid mechanism.

The proposed system will be implemented using Ethereum blockchain technology and smart contracts. We will evaluate the performance of the proposed system in terms of security, scalability, and efficiency using simulation and real-world experiments.

In summary, the goal of this proposed work is to create a decentralized trust management and secure voting system that uses blockchain technology and offers a transparent, safe, and effective platform for voting and trust evaluation. The proposed system has the power to fundamentally alter the way we manage trust in a variety of applications and during elections.

B) Registration & Configuration

A user must first register with the system in order to be eligible to vote. The voter registration mechanism is shown in Fig. 2. The user's MSISDN (phone number) is automatically retrieved by the application when it is first launched from the Subscriber Identity Module (SIM card). Because transactions to the blockchain cost GAS, which is priced in ether, registration and voting require the EOA to have enough of the cryptocurrency. The program creates a blank Ethereum wallet and asks the user to add funds using the wallet management function method as detailed in

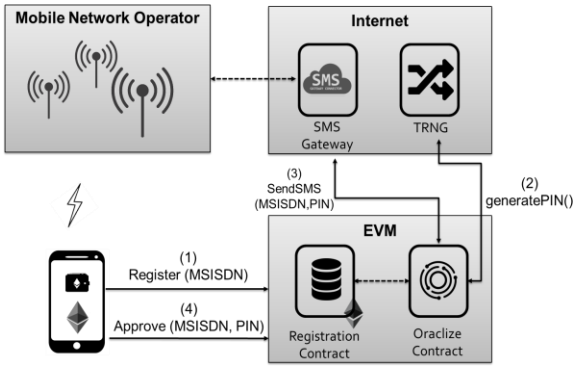

Fig 2: Election Process & Voter Registration

V. IMPLEMENTATION AND RESULTS

We put the proposed solution into practice using a variety of technologies to validate the system. Solidity, a contract-oriented programming language, is used to create the voting and registration smart contracts. NodeJS server-side scripting is used to interface with the event management server. The Blockchain network is simulated using the MetaMask.

LOGIN

Web3 apps replace the need for a username and password for authentication with a wallet-based system. The private key is used for authentication, while the public key is used to uniquely identify the account holder. Our voting web app makes use of the meta mask wallet, a plug-in for many web

browsers. In order to access the app, the user needs just link it to a payment account stored in the user's digital wallet. The suggested system is designed such that each voter needs only one login. The key features of this system are its privacy protections, its one-vote-per-mobile-phone-number voting policy, and its commitment to data accuracy and openness.

INITIATING A NEW BALLOT

A new ballot may be initiated by any user by providing ballot details and authorizing the transaction using the wallet. With the blockchain network's approval, the transaction is added to the permanent record. The person making the ballot must include a list of valid addresses (the public addresses of user accounts).

VOTING PROCESS

Users who are of voting age can do the same thing using a meta mask to link their accounts. After a search for a matching voter, a list of candidates that are up for election will be displayed, along with the opportunity to vote against each of them. If, however, there is no successful match, access will be terminated immediately. When a user approves a transaction in their wallet, their vote is added to the distributed ledger at the same time the transaction is broadcast to the network. To this aim, each valid vote counts as a separate transaction on the voting app's blockchain.

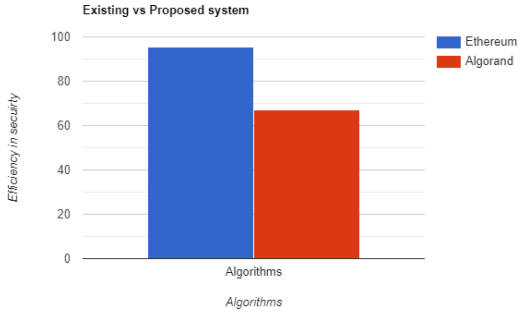

Fig 3. Ethereum Usage

While both Ethereum and Algorand are capable blockchain platforms that support the development of decentralized applications and smart contracts, Ethereum has several advantages over Algorand.

Established ecosystem: Ethereum has been around since 2015 and has a well-established ecosystem of developers, dApps, and users. This means that there are more resources available for developers looking to build on the platform, including documentation, tutorials, and support from the community.
Established DeFi ecosystem: Ethereum has a well-established DeFi ecosystem, with numerous decentralized exchanges, lending platforms, and other financial applications built on the platform. This ecosystem has a lot of liquidity and is well-established, making it easier for users to access DeFi applications.

More advanced smart contract capabilities: Ethereum has more advanced smart contract capabilities than Algorand, with a more robust programming language (Solidity) and more complex smart contract functionality. This makes Ethereum a better choice for complex applications such as DeFi, where advanced smart contracts are needed to support complex financial transactions

The web page that event planners use to add a new voting event is depicted in Fig. 4.

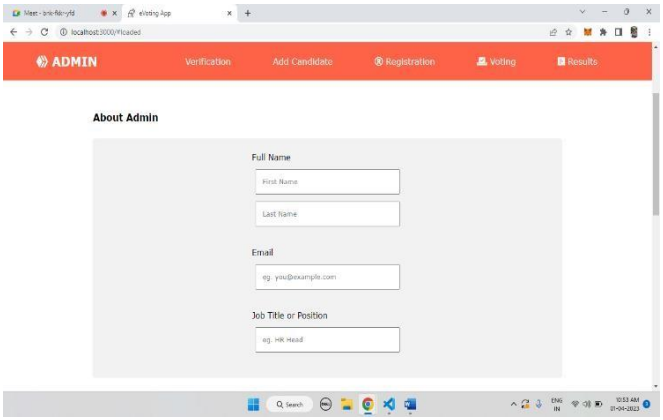

Fig 4. Organizing a New Election

The voting results dashboard is shown in Fig. 5 for event organizers to see.

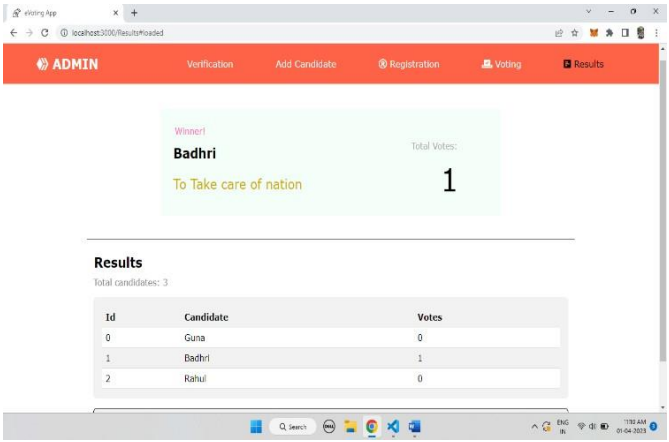

Fig 5. Instantaneous Results Visualization

A user could register with the system in two to four minutes. This amount of time is only used once during configuration. Voting, on the other hand, took between 40 and 2 minutes. This much time is spent on each vote.

VI. CONCLUSION

Blockchain was implemented as a network-basedelectronic voting system. This system will become accustomed to using blockchain as an integrated system and database to collect and store voter information or credentials that will be used for their authentication. Details about the candidates or voters will be used by the system during the voting process. The management of voting procedures and results will be attributed to smart contracts. Our system improves the effectiveness of verifying and awarding a candidate's vote. By encrypting the vote, blockchain technology makes it impossible to tamper with any votes. It makes sure that a voter can only cast one ballot for a candidate. Election results are quickly retrieved by the system, which lowers labour costs and counting errors.

REFERENCES

[1] Nakamoto Satoshi, Inventing bitcoin, implementing the first blockchain, deploying the first decentralized digital currency "A Peer-to-Peer Electronic Cash System" original 20 March 2014.

[2] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management." In Open and Big Data (OBD), International Conference on, pp. 25-30. IEEE, 2016.

[3] Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, Computer Networks: The International Journal of Computer and Telecommunications Networking,December 2017.

[4] Nakamoto Satoshi, Inventing bitcoin, implementing the first blockchain, deploying the first decentralized digital currency "A Peer-to-Peer Electronic Cash System" original 20 March 2014.

[5] Nicole J. Goodman;Jon H. Pammett , 2014. "Internet Voting in a Local Election in Canada", in Internet and Democracy in Global Perspective, Studies in Public Choice 31, Eds. Bernard Grofman, Alex Trechsel, and Mark Franklin, Springer Verlag.

[6] Rafer Cooley;Shaya Wolf;Mike Borowczak Conference: 2018 IEEE International Smart Cities Conference (ISC2)

[7] Guo, Ye, and Chen Liang. "Blockchain application and outlook in the banking industry." Financial Innovation 2, no. 1 (2016): 24.

[8]Ikhsan Darmawan E-voting adoption in many countries: A literature review,First Published October 12, 2021

[9] R.S. Yashank E-Voting System using Hyperledger Sawtooth , Communication & Materials (ICACCM), 2020 International Conference on

[10] E-Voting Systems using Blockchain: An Exploratory Literature Survey, 2020 Second International conference on Inventive Research in Computing Applications (ICIRCA)

[11] . L. Meeser, "Decentralized, transparent, trustless voting on the ethereum blockchain," 2017.

[12] P. McCorry, E. Toreini, and M. Mehrnezhad, "Removing trusted tallying authorities," Technical report, Newcastle University, 2016. Cited on, Tech. Rep., 2016.

[13] D. Orenstein, "Quickstudy: Application programming interface (api)," 2000.

[14] V. K. Katankar and V. Thakare, "Short message service using sms gateway," International Journal on Computer Science and Engineering, vol. 2, no. 04, pp. 1487–1491, 2010.

[15] E. F. Kfoury and D. J. Khoury, "Secure end-to-end voip system based on ethereum blockchain," Journal of Communications, vol. 13, no. 8, pp. 450–455, 2018.