2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) | 979-8-3503-1912-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SMARTGENCON60755.2023.10442887

Ether Vote: Revolutionizing Elections with Blockchain-Powered Electronic Voting System

Sijo Joseph
M.Tech Scholar
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi, India
sijojosephmrs@gmail.

Priyank Pandey
Department of Computer Science & Engineering
Graphic era deemed to be university,
Dehradun Uttarakhand, India
Priyankpandeyrc@gmail.com

Manju Khari
Professor
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi, 110067, India
manjukhari@yahoo.co.in

Kapil Kumar
Ph.D scholar
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi, 110067, India
kapil.sharma0942211@gmail.com

Piyush Pratap Singh
Associate Professor
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi, India
piyushpsingh@mail.jnu.ac.in

***Abstract*— Voting is a crucial part of democracy because it gives people the chance to voice their opinions, hold elected officials responsible, encourage diversity in the government, cultivate civic participation, and defend themselves from tyranny. Existing electronic voting (e-voting) systems do in fact suffer a number of important obstacles, with security difficulties and a lack of transparency ranking as two of the most important problems. Given the significance of elections in democracies and the likelihood of fraud or other forms of manipulation in electronic voting procedures, these issues are extremely pressing. Systems used for electronic voting heavily rely on software, which might occasionally have vulnerabilities that hackers can exploit. Any weak point in the system can be used to sway elections or jeopardize its security. To address these issues, a strong, secure electronic voting system (EVS), an open system design, impartial audits, and a dedication to inclusion and accessibility are required. For democratic processes to continue to be trusted and the right to vote to be protected, e-voting system integrity must be ensured. It is necessary to create a new Electronic Voting System (EVS) that can offer greater security, speed, and accuracy than the EVS used in the past. The authors of this research suggested a blockchain-based secure EVS. Immutable, transparent, and secure distributed ledger technology named as blockchain. Blockchain used to implement an E-Voting system that is transparent, tamper-proof, and can guarantee the correctness and integrity of the voting process.**

Keywords—Blockchain, Voting, Ethereum, EVS.

I. INTRODUCTION

As members of the largest democracy on Earth, authors understand the significance of voting and the need of a modernized and efficient voting system in light of recent technological advancements [1]. Existing systems be either a ballot or Electronic Voting Machine (EVM), which is time consuming in both the voting and counting process, and uncomfortable to most people, [2], which affect the polling percentage as well. In addition, there are various allegations of EVM that is tempered. Traditional voting procedures might make people uncomfortable, especially in crowded polling places. People could have to stand in queue for a long time, which could cause physical pain and voter fatigue [3]. Voter turnout may be significantly impacted by the inconvenience and discomfort associated with traditional voting methods. These obstacles may discourage many people from taking part in the political process, which would diminish the polling percentage [4].

The authors emphasize the pressing requirement for an advanced and effective voting system that considers these issues. Such a system would take use of technical developments to make voting more convenient, secure, and open to all citizens.

A. Problem Statements

Traditional EVSs indeed face several significant challenges, with security concerns and a lack of transparency being two of the most critical issues. These challenges are especially pertinent given the importance of elections in democratic societies and the potential for fraud or manipulation in electronic voting processes.

a) E-voting systems rely heavily on software, which can have vulnerabilities that hackers can exploit. Even a small flaw can be misused to manipulate votes or compromise the system's security. Addressing these challenges requires robust secure Electronic Voting System (EVS), transparent system design, independent audits, and a commitment to inclusivity and accessibility.

b) Ensuring the integrity of e-voting systems is essential for maintaining trust in democratic processes and protecting the fundamental right to vote. Therefore, an effective, secure, and advanced voting system is the need of hour to provide more security efficiency, speed, and accuracy compared to traditional method EVS. In this paper, authors proposed a secure EVS based on Ether Vote using EVS. Blockchain is a distributed ledger technology that is immutable, transparent, and secure. By using blockchain for E-Voting, it is possible to create a tamper-proof and transparent system that can ensure the accuracy and integrity of the voting process

979-8-3503-1912-5/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

B. *Structure of Voting System & Considered Objectives*

The basic structure of a voting system is on three different groups, the candidates, the voters, and the agency who are having it conducted. Here the agency that is going to conduct the election. In a system the basic thing agency have to ensure is the trust from two other parties, so that few basic concerns need to consider.

a).Authenticity of voter: The voter should be eligible for the election, for example in Indian system, who is a citizen of India who is at least 18 years old, and enrolled for a particular constituency [5].

b).Anonymity of Voter: even though users must confirm the vote is recorded it should not be recorded in such a way that any second party can map a person with a vote [5].

c).Authenticity of Candidate: List of Candidates must be managed by the agency who is conducting the election, In Indian Situation, The Election Commission of India [6].

d).System being tamper-proof: Once a vote is made, it should not be changed at any cost. In addition, there should be only one way to vote which is via authenticity of voter. Even the Agency, which conducts the election, cannot cross this line [6].

C. *Research Objectives*

To handle the issues in current voting system and to achieve considered objectives are following:

a) The authors propose decentralizing voter registration and validation procedures, appropriate voter validation utilizing IDs, making voting data integral and irreversible, building the system in a trustworthy and resilient environment, and finally a straightforward and user-friendly user interface for both voting and the counting process. A cutting-edge concept called blockchain, on the other hand, employs consensus methods, protocols, and cryptographic functions to enable network decentralization without a single point of failure.

b) Software developers may use the open-source Ethereum Blockchain, which features a Turing-complete scripting language, to create dApps that benefit from the distribution aspect of blockchain.

c) Subsequently, the following blockchain functionalities will be present in dApps:

    a) Integrity of Data

    b) Processes of consensus have decentralized verification and oversight.

    c) Run-time environment with transparency.

    d) Runtime environment with public business rules.

    e) Availability.

In this work, authors propose a decentralized voting system based on Blockchain Technology to solve the existing problems of traditional E-Voting systems. This scheme uses a cutting-edge technique to secure the EVS.

II. LITERATURE REVIEW

The issues with the existing Electronic Voting System (EVS) have been explored in a number of research articles by the authors. The goal of the articles is to secure the present EVS utilizing blockchain and a perfect voter authentication mechanism. A few significant studies that have been examined are listed below:

The authors give a thorough description of their e-voting system, including how it was implemented on the Multichain platform, in article [7]. The scheme's capacity to construct a completely verifiable e-voting system is confirmed by the paper's extensive evaluation of the plan.

To address shortcomings in existing systems, the author of article [8] offers a novel electronic voting method that makes use of blockchain technology. In order to construct an electronic voting system based on blockchain, the article also evaluates alternative blockchain frameworks.

The main goal of paper [9] is to evaluate the various uses of blockchain as a service for putting distributed electronic voting systems into place. Others of these applications have been successfully implemented in the actual world, while others are still in the conceptual stage. By using a blockchain-based electronic voting system, expenses are further decreased while security and privacy are improved.

Designing a decentralized e-voting system is the main goal of this study [10]. The main idea entails combining blockchain technology with covert sharing protocols and homomorphic encryption to produce a decentralized electronic voting programmed that functions without the aid of a reliable third party. In addition to protecting voter confidentiality, data transmission privacy, and the verifiability of ballots throughout the billing phase, this solution guarantees a transparent voting procedure for the public.

In article [11], the authors present a technique to emphasize security by combining a sharding mechanism with the PSC-Bchain hybrid architecture. The efficiency and scalability of the blockchain-based electronic voting system are enhanced because of this integration. The authors also compare and contrast attack scenarios on conventional blockchain and their hybrid blockchain, evaluating the security features. They get new knowledge on the general security, functionality, and scalability of blockchain-based electronic voting systems because of their tests.

The study in [12] evaluates current blockchain-based electronic voting platforms and develops a blockchain-based vote recording system. This technology is intended to guarantee the voting process' immutability, dependability, and openness. The suggested solution successfully tackles the issue of vote manipulation by using a cryptographic hash function to secure transactions added to the blockchain, making it nearly difficult to change votes recorded in the blockchain and making them unchangeable.

The author [13] in this study suggested a blockchain-based electronic voting system. Because it is decentralized, the system does not rely on trust. Voting will be possible on any Internet-connected device by any registered voter. No one will be able to tamper with the Blockchain since it will be spread widely and publicly verified.

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

III. RESEARCH GAP

Authors found certain gaps in existing research, which explore by various researchers that are following:

a) The study of the potential of blockchain technology for safe and transparent e-voting is still in its early stages. This entails investigating and evaluating the utility and security of blockchain-based voting systems.

b) A deeper comprehension of the dangers and risks related to electronic voting methods is crucial. Designing countermeasures and identifying vulnerabilities can be aided by developing systematic frameworks for risk assessment and threat modelling.

c) There is a constant need for research into creating and evaluating end-to-end verified electronic voting systems. Voters may independently confirm that their votes were accurately recorded and tallied using these techniques, which increases openness.

IV. PROPOSED WORK

In proposed work, authors are going to develop Blockchain based Election Voting System (EVS) to resolve the existing issues found in existing systems of voting. For developing authors used four components of system as named are web App, mobile App, application server, smart contracts, SMS Gateway, and Foul proof Face ID to develop blockchain based EVS.

The web app enables event organizers to design and plan fresh voting activities Within the blockchain network, each voting event is represented by a different and unique Smart Contract. The administrator enroll the list of all candidates before starting an HTTP request to the server with the entered information. This Web and Mobile app's goal is to serve as an API interface for application programming, allowing anyone to create new voting events.

The idea behind the application server is to publish the smart contract to blockchain network along with the data that was obtained from the web and mobile app. Hence, it needs a full ethereum network interface node, an ethereum wallet, (address) needed to deploy the contract, and a db to store the list of addresses(contract) that will subsequently be queried by the app. The smart contract is deployed only once, whatever being the voting cases it cannot be repeated which makes sure an voter will be registered only once, same for the candidates.

Vote written only once and deployed several times making the voting process happen, Data for the voting event define only by admin. Using these two smart contracts authors designed the voting process which can make a transparent, decentralized system keeping the anonymity of the process. Anonymity is achieved by never storing or mapping voter information with the recorded vote. Once the vote is recorded it will only keep the value of vote but no the information about the voter, by not sharing the same value. SMS Gateway(MSISDN and OTP) connects to the application server at the time of registration and voting It produces an OTP (One Time Password), Users have to enter the same once as it Receive in the phone, It increases the level of security in most cases since it is linked with AADHAAR like systems it can be a source for biometric details.

In order to establish a Foul-Proof Face ID system for voting, a face recognition model deploy to ensure that the individual who has registered with their voter ID is indeed the one casting the vote. This measure is imperative for bolstering the security of the voting process. Nevertheless, there is a significant limitation associated with conventional facial recognition techniques, namely their susceptibility to manipulation with a victim's image or video.

To address this vulnerability, the authors have developed a real-time liveness detection method aimed at preventing such fraudulent activities. This method introduces an additional layer of security by requiring voters to perform random facial gestures, such as smiling, turning left or right, or blinking their eyes, in real-time. Prior to casting their vote, each user mandate to execute three such random gestures. If the system's liveness detection fails to recognize these gestures, the user will be unable to proceed with voting. They must sign in once more to ensure the integrity and authenticity of their identity, thus enhancing the overall security of the voting process.

The face authentication process, authors of the paper utilizes Haar Cascade Files to assess the liveliness of the face and subsequently compares the facial data with the uploaded image. When a user attempts to vote, the camera activates and prompts the voter to perform three random facial gestures. If these gestures are successfully completed, it confirms the liveliness of the user, and then the facial data is matched with the registered user's photograph. This ensures both the user's liveliness and the authenticity of their identity, allowing them to proceed with voting.

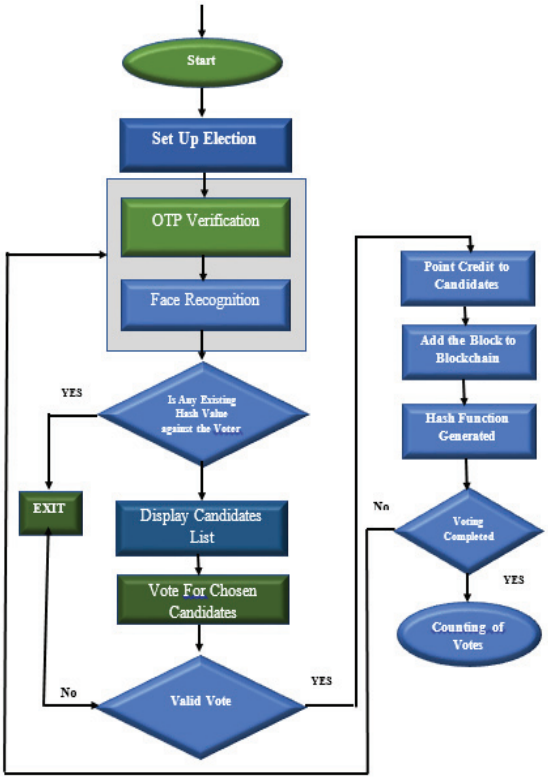


Fig. 1. Flow chart of voting process.

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

As above figure 1, describe the process of voting in which system initialize with candidate and voter details, Election Time, Date etc. For Authenticating Voters need any ID card than can be used to authenticate the user initially, at the voting time user will have to use their OTP and the face detection for getting eligible to vote. Hash Value already existing against any Voter’s name, therefore, if the voter's authentication is successful, a hash value will be looked up against the voter's name. The hash value deploy to the voter for casting a vote; otherwise, there will not be one, if the hash value is present, the voter will not be allowed to vote again. A list of the candidates in the voter's constituency is display if they have not yet voted; Voter's ID number is applied to retrieve information about the constituency. From the list voter choose their choice of candidate. When all conditions are satisfied, it counts as a valid vote

Points credited and added consequently to the candidate account as a legitimate vote cast. There is one attribute for each candidate that maintain in order to keep the votes coming in. This will make it easy to display the results.

Blockchain of community added with new block in which a block is formed for each legitimate vote that includes the voter's name, the recipient of their vote, the time the vote was cast, and the previous block's hash.

Generating Hash value against that Voter’s name in which a hash value generate against the voter’s name once block add. Vote recorded step verify whether the voting has been finished.

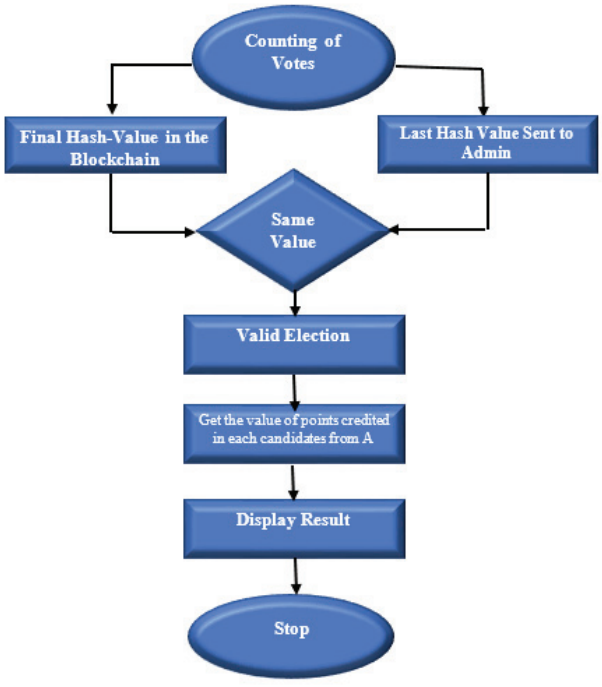

Counting of Votes
Final Hash-Value in the Blockchain
Last Hash Value Sent to Admin
Same Value
Valid Election
Get the value of points credited in each candidates from A
Display Result
Stop

Fig. 2. Flowchart Process of Counting,

As seen in figure 2 the system continues to receive votes if it is not finished; if it is, it will continue by updating counter value of the candidates' account. The most recent produced hash send to the admin upon the end of voting: Getting the Value of Points from Blockchain (Created to Each Candidate). The entire amount of points given to each candidate uses to calculate their vote total, and this information pull from the blockchain used for electronic voting.

After the counting of votes Result is displayed different visualization techniques are also included for better communication. To prevent attack 51%, this framework to make voting system transparent using blockchain technology suggests.

V. DATA DESCRIPTION

In this study, authors perform comprehensive collection of data related to an electronic voting system that leverages blockchain technology to ensure the integrity and security of the voting process. This dataset design to support research, analysis, and development in the field of electronic voting systems and blockchain technology. Collecting data for an e-voting system using blockchain involves various aspects, including voter registration, voting transactions, liveness detection, and security logs [7].

The dataset include Voter information, Voter ID, Name, Address, Age, Voter Registration, Status, Voting Transaction Data, Transaction ID, Timestamp, Blockchain Block Number, Candidate voted For, Vote confirmation (Success/Failure), Blockchain information such as Blockchain Blocks, Transactions within Blocks, Smart Contracts Used, Block Timestamps, Liveness Detection Data that include Facial Gesture Data (e.g., smiling, turning left/right, blinking), Liveness Confirmation (Success/Failure), Security Logs that involve Authentication Logs, Security Incidents (if any), Identity Fraud Attempts , Voting Outcome Data that involve candidate Names, Vote Count for Each Candidate , Election Results , User Interaction Data that involve User Interactions with the Voting Application, Actions Performed (e.g., registering, voting, liveness confirmation)[7-8].

The dataset organize into structured tables and logs. It includes voter information, voting transaction records, blockchain data, liveness detection records, security logs, voting outcomes, and user interactions. Each table or log provide in a standardized format, typically in a CSV or JSON file, allowing for easy analysis and processing [9-10].

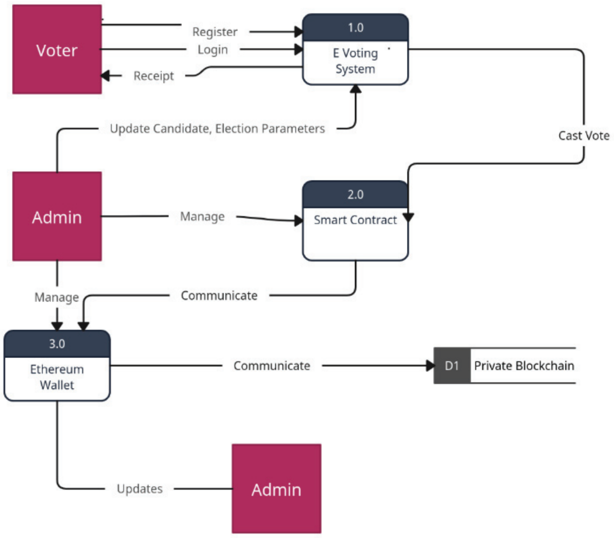


Fig. 3. Data Collection Process.

As depicted in figure 3 the data collection process description for the proposed work. As voters register into the system and receives a secret key as the receipt of successful

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

registration. The admin has the privilege to update the candidates and other election parameters. Voters then uses this secret key as the identity to cast their vote. Vote update in the blockchain via smart contracts, which in turn depends on an Ethereum wallet for transaction. Miners at Ethereum, checks the blocks containing voting data and accepts the block if consensus is reached [10-11].

Voter Registration means collect voter information when individuals register to vote. This data includes names, addresses, and other personal details. Voter ID creation assign a unique voter ID to each registered voter and store it securely in the system. In similar fashion, authors collect data via Voting Transactions, Liveness Detection, Security Logs, Voting Outcome Data, User Interaction Data, Blockchain Data, Demographic Data, and System Logs [12].

VI. RESULT AND IMPLEMENATION

Authors used smart contract to implement and it is self-executing digital contract that automatically upholds and facilitates the conditions of an agreement between parties. Agency created a smart contracts using Solidity, which is the programming language of Ethereum.

The smart contract contains functions for changes in blockchain. In Solidity, smart contracts can make by basic codes. There are two types of transactions present, payable, and non-payable For example; a transaction that modifies the block chain's state by increasing the number of votes cast when a voter casts a ballot is a payable function, whereas a transaction that verifies the amount of votes cast is a non-payable transaction [13-14].

In order to cast a valid vote, a user must first register with the system. Users must submit their name, voter ID, and constituency when registering. The programmer creates an Ethereum wallet for each user. Together with other functions, the register function is available. The web application makes use of these functions. A request is made to the server upon calling. The server has the ABI that connects the smart contract. The server performs the function using the ABI and the data from the request and the blockchain update as a result. As explained in proposed model no details of voter is being recorded in this process it can only make a voter ineligible to vote again after one vote, since vote is not being mapped to any voter, this system keeps the anonymity of the voter at the same time keeping transparency[14].

Authors used a new framework 'Eth-Brownie' for compiling and deploying smart contracts; "Brownie" is a popular development framework for Ethereum smart contracts. This makes creating, evaluating, and implementing smart contracts on the Ethereum Blockchain simpler. It is a python-based development environment and it includes a number of tools and features to speed up the process of creating smart contracts. Because of the same using Brownie Authors integrated solidity code with python, solidity running inside python made it easy to develop a web app as UI, etc. Authors used Django 4.0 framework to structure application backend and connect it with a front app, which is HTML+CSS [14].

A high-level Python web framework for creating web apps called Django makes the same easy. The Model-View-Controller (MVC) architectural pattern is used, and they do not repeat principle emphasize. With the large range of tools and functionalities that Django offers, developers can concentrate on creating application logic rather than worrying about low-level implementation concerns. Django is a well-liked option for creating web applications due to its adaptability, thorough documentation, and active community support. It frequently used to create many different kinds of applications, including social networks, e-commerce platforms, Content Management Systems (CMS), and more [15].

The process of face authentication and liveliness verification in an e-voting system using Haar Cascade Files and random gestures involve face authentication with Haar Cascade files in which the initial step of the e-voting system, the user's identity confirm via facial authentication. Haar Cascade Files are used to detect and classify key features on the user's face, such as eyes, nose, and mouth. This step ensures that the person attempting to vote is indeed the registered voter associated with the provided voter ID [14-15-16].

After the initial facial authentication, comparison with uploaded image for that system compares the facial features extracted from the user's live image with the facial data from the registered photograph associated with the voter's ID. This procedure makes that the face being shown is the same as the one in the registration-related photo. The system starts a liveliness verification stage to increase security even further and stop false voting. This is done to make sure that the user is actually there and actively taking part in the voting process, as opposed to being impersonated by a still image or video. The camera opens when the user tries to cast a ballot, asking them to make three random facial motions. Smiles, head turns to the left or right, and eye blinks are a few examples of these movements. These motions are unpredictable, making it difficult to record or mimic them [15-16].

To verify that user activities are real-time, the system examines their analysis. It verifies that the user's behaviors are consistent with those of a real person actively engaging in the voting process and that the random gestures are effectively carried out. This procedure makes that the voter is actually present during the voting process. Once the random motions have been successfully completed, the system once more compares the user's registered photo to the live facial data. This step is essential to ensure that the voter who began the voting process is the same voter who is registered to vote. The system verifies the user's identity and liveliness when the liveliness verification and face data matching are both successful. This indicates that the individual trying to cast a ballot is not only a registered voter but also present in person and actively taking part in the voting process [15].

The user is given permission to continue the voting procedure after their liveliness and validity have been verified. The e-voting system is made more resistant to fraud and unauthorized use thanks to this multi-step authentication procedure, which guarantees its security and integrity. In conclusion, the integration of Haar Cascade Files for facial authentication, random gestures for liveliness verification, and comparison with the registered photograph creates a robust and secure system where the liveliness and authenticity of the voter are confirmed, thus enhancing the general security and integrity of the e-voting process[16].

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

Additionally, the authors have used a local blockchain to test the Deep Face Library application. Specifically, they have chosen to use Ganache, which is a popular Ethereum Blockchain simulator. This choice of a local blockchain simulator like Ganache indicates a commitment to ensuring the security and reliability of the voting system by testing it in a controlled and simulated blockchain environment before deploying it in a live voting scenario [14-15-16].

In conclusion, the Deep Face Library's incorporation of cutting-edge facial recognition models and its high accuracy on the dataset demonstrate its effectiveness in facial recognition tasks. Using Ganache as a local blockchain simulator reflects the authors' dedication to thoroughly testing and securing the e-voting system before real-world implementation. This combination of technologies and methodologies contributes to a robust and secure e-voting application.

As main objective of the authors to make system secure and reliable. Researchers created a successful blockchain EVS, which eliminates dual voting, and vote rigging. Apart from that, researchers also created a strong authentication system that detects identity fraud

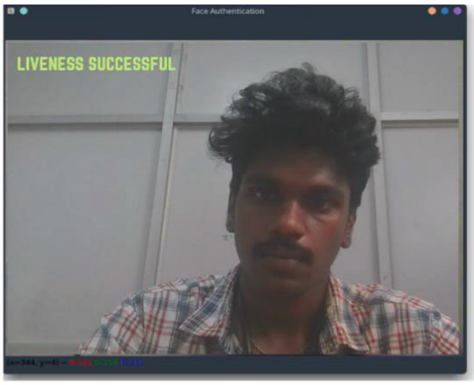
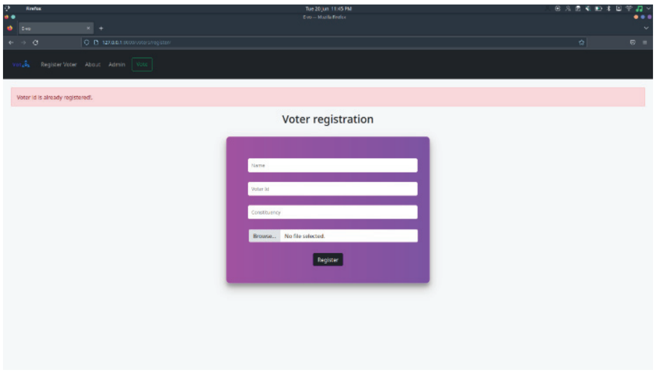


Fig. 4. Liveliness Verification



Voter id is already registered!.

Voter registration

Fig. 5. GUI of Vote E

As seen in figure 5 represent the graphic user interface (GUI) of proposed system. Authors have tested the voting system for all scenarios like repeated voter registration, invalid votes, registration after starting election etc. and voting system found to be reliable in conditions.

VII. PERFORMANCE ANALYSIS

The Performance Analysis involves assessing how well something has performed or evaluating its effectiveness.

TABLE I. PERFORMANCE ANALYSIS OF PROPOSED SYSTEM

"No of Voters"	*"Correct Verification"*	*"Correct Count"*	*Voting*	*"Accuracy"*
4	4	4		97%
6	6	6		97%
8	8	8		97%
15	15	15		97%

In this context, the table labeled as Table 1. Presents various parameters that are crucial for analysis of proposed system.

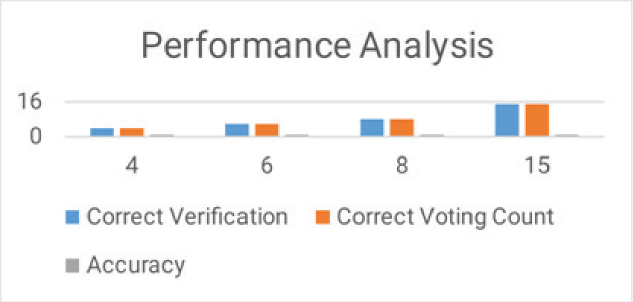


Fig. 6. Performance Analysis via Graph.

As figure 6 represents the performance analysis of proposed system via graph and representing results in terms of accuracy, which is attained 97% in each use cases. The obtained result is higher than result of existing.

VIII. CONLUSION

In conclusion, authors proposed and implemented decentralized E-Voting System using blockchain components. Conventional voting system being outdated, expensive, and slow it leads to different problems including wastage of resources and fall in polling percentage. At the same time existing E- Voting systems, which are centralized, and having, many security issues are not considered as an alternative. That is where the need of a voting system based on blockchain. Being on blockchain the voting system is Decentralized, Immutable, Transparent and Secure, the only question comes up with transparency is of anonymity, with algorithms. Authors could ensure the anonymity of a voter. Included with a proper authentication system that ensures the liveliness and authenticity of voter, and considering data is immutable, this can be an efficient and better existing voting system.

REFERENCES

[1] J A Samsul, & M B Limkar, "A biometric-secure cloud based e-voting system for election processes", International Journal of Electrical and Electronics Engineering Research (IJEEER), 4(2), 2014,145-152., Chicago.

[2] A Nadaph, R Bondre, A Katiyar, D Goswami, & T Naidu, "An implementation of secure online voting system", International journal of engineering research and general science, 3(2),2015, 1110-1118.

[3] M S Farooq, U Iftikhar, &A Khelifi, "A framework to make voting system transparent using blockchain technology", IEEE Access, 2022, 10, 59959-59969.

[4] G Rathee, R Iqbal, O Waqar, & A K Bashir, " On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities", IEEE Access, 2019,9, 34165-34176.

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.

[5] N Gailly, P Jovanovic, B Ford, J Lukasiewicz, & L Gammar, “Agora: bringing our voting systems into the 21st century”,2018,pp.1-6.

[6] A Parmar, S Gada, T Loke, Y Jain, S Pathak, & S Patil, “ Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP”, In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) ,2021, pp. 1-5, IEEE.

[7] KM Khan, J Arshad, MM Khan, Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR)*, 2018, *14*(1), 53-62.

[8] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson, Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 2018, pp. 983-986). IEEE.

[9] S Al-Maaitah, M Qatawneh , Abdullah Quzmar, E-voting system based on blockchain technology: A survey. In *2021 International Conference on Information Technology (ICIT)* (pp. 200-205). IEEE.

[10] JH Hsiao, R Tso, CM Chen, ME Wu , Decentralized E-voting systems based on the blockchain technology. In *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17*, 2018, pp. 305-309. Springer Singapore.

[11] A Y Abuidris, R Kumar, T Yang, J Onginjo , Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Etri Journal*, 2021, *43*(2), 357-370.

[12] S Agbesi, G Asante, Electronic voting recording system based on blockchain technology. In *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)* (pp. 1-8). IEEE.

[13] AB Ayed, A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 2017, *9*(3), 01-09.

[14] A Baobaid, M Meribout, VK Tiwari, & J P Pena, “ Hardware accelerators for real-time face recognition: A survey”, 2022, pp.1-10,IEEE Access.

[15] A Atri, A Bansal, M Khari, & S Vimal, “De-CAPTCHA: A novel DFS based approach to solve CAPTCHA”, schemes. *Computers & Electrical Engineering*, *97*, 2022,1-10.

[16] M Khari, M Kumar, S Vij, & P Pandey, “ Internet of Things: Proposed security aspects for digitizing the world”, In *2016 3rd international conference on computing for sustainable global, pp-1-6.*

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on March 30,2025 at 08:30:15 UTC from IEEE Xplore. Restrictions apply.