



DECENTRALIZED E-VOTING SYSTEM USING BLOCKCHAIN

¹ Dr S Gayathri Devi, ² R Sugavaneswara, ³ G Sanjay Balan, ⁴ P Sriramprasad,

¹ Associate Professor, ^{2,3,4} Student,

^{1,2,3,4} Department of Computer Science and Engineering,

^{1,2,3,4} Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India.

Abstract: There is no guarantee that the votes cast will reach the appropriate candidate or that there are no tampering attempts in place with the current voting system. Voters encounter two main issues: long lines at polling locations and difficulty voting for voters who are out of town. These issues lead to a significant decline in the percentage of voters who cast ballots. As an online voting system that lets voters to cast their ballots from anywhere and avoid crowds and other issues, the proposed helps users authenticate their votes and makes it extremely difficult or impossible for any hacker to penetrate the system.

IndexTerms - Blockchain, Smart Contracts, Electronic voting, Privacy, Ethereum. MetaMask, Ether, REMIX-IDE.

I. INTRODUCTION

The problem with a centralized environment is that if the data in the centralized medium, such as the database, is changed, then all of the user's data changes as well. The proposed work gives users access to a fully decentralized network that lacks any centralized medium to store their data. Blockchain is utilized to create this safe decentralized system. Blockchain is a decentralized system in and of itself; it is a component of web3, which encourages decentralization.

Because blockchain is developed using safe techniques like cryptography, decentralized networks, and peer-to-peer networks, it is regarded as one of the most trusted and secure platforms for transactions (in this case, voting). This ensures that users have a high level of trust in the platform.

With a significant risk of data exposure, blockchain makes sure that the system has no central hub or centralized medium. It is an entirely open, cost-free, decentralized network with excellent privacy and transparency. Data that is added to the blockchain network is permanent and unchangeable.

Think of this as an illustration of the blockchain network. If your school, college, or other institution has a centralized method for publishing results, and a student knows how to hack into the system to alter the outcome, this would be simple for the student to do so since all they would need to do is break through the one centralized network. However, if the same scenario were to occur in a decentralized system or blockchain, the student would have to solve every previously used block. For example, if another student had already opened a block to see the outcome, the hacker would also need to access that student's data. What would happen if ten, fifty, or more students opened blocks?

These are some statistics on the general elections held in India: just roughly 67% of the country's eligible voters cast ballots, with 33% not doing so. Nearly 68% of those who do not vote report having one of the following problems: a long queue at the polls, transportation difficulties, lack of availability at the polling place, or a lack of trust in the voting process. Voters will feel more like democratic citizens and be able to cast their ballots more frequently thanks to the online decentralized voting method.

This study focuses on the development of a blockchain-based decentralized voting application and examines prior research in this area as well as methods for assessing the suggested work. talks about the software and technologies that were used to construct the project as well.

II. LITERATURE SURVEY

Syada Tasmia Alvi; Mohammed Nasir Uddin' Linta Islam; et al. [1] designed this voting system to ensure stability and foster engagement and credibility among the electorate, alongside fair polling data and tamper-resistant vote counting, a blockchain-based digital voting system using smart contracts was developed. Three smart contracts execute various election operations, minimizing third-party involvement compared to existing systems. Encrypted casted votes remain inaccessible until the election concludes, ensuring voter-vote anonymity. Voter information is stored as hashes, preserving anonymity and reducing costs. Post-election,

voters can verify their votes using unique vote IDs received during casting, enabling global participation via smart devices. This inclusive approach aims to bolster voter turnout worldwide, promoting democracy in all regions.

Prajwal Shiwal; Dhruv Morey; Harshad Shivankar; et al. [2] proposed a Ethereum-based electronic voting system based on blockchain technology. It demonstrates how centralised voting systems' drawbacks can be solved by blockchain technology. Voter accounts, candidate details, and votes are stored in this version using a database and the Ethereum blockchain as a network. Smart contracts are used in this implementation. People want a less confusing system that is crystal clear and ensures that their data is safe and secure. Blockchain technology holds great promise for solving many real-world problems associated with relying on third-party centralised authority in day-to-day life.

Kriti Patidar; Dr. Swapnil Jain [3] presented a Ethereum-powered electronic voting system based on blockchain. It demonstrates how blockchain technology can get around centralised voting methods' drawbacks. This implementation stores voter accounts, candidate information, and votes in a database and using the Ethereum blockchain as a network. In this implementation, smart contracts are utilised. The virtual client is used to test this implementation.

Electronic voting systems need to handle a number of issues with data privacy and integrity, transparency, verifiability, and authentication, according to Uzma Jafar, Mohd Juzaidin Ab Aziz, Zarina Shukur, et al. [4]. Blockchain technology, however, offers an innovative solution to many of these problems.

Yousif Osman Abuidris; Rajesh Kumar; Wang Wenyong [5] designed a system Based on the survey, blockchain technology has garnered a lot of attention lately as a distributed, decentralised public ledger in a peer-to-peer network. With the use of a linked block structure and a reliable consensus process, this technology enables the creation of a tamper-proof digital platform for the exchange and storage of data. Blockchain technology is thought to have applications in a wide range of interactive online systems, including voting, supply chain, and Internet of Things platforms.

Friðrik Þ. Hjálmarsson; Gunnlaugur K. Hreiðarsson; Mohammad [6] introduced a smart contract-based blockchain electronic voting system that ensures voter anonymity while facilitating safe and economical elections. They have demonstrated how blockchain technology presents a fresh opportunity to get around the drawbacks and adoption hurdles of electronic voting systems, ensuring election security and integrity and establishing a foundation for openness.

Naina Nagesh Dhepe and Dr Pathan Mohd Shafi [7] state that the main goal of the suggested system was to combat electoral fraud and errors. With a population of over one billion, India is the largest democracy in the world. It has 543 parliamentary constituencies and over 668 million electors. The link between the governed and the government is voting. The use of technology in the voting process has received more attention in the past few years. There are numerous security flaws in the current voting system, and it is challenging to establish even basic security features.

M. Sai Sathwik¹, G. SaiPrasad¹, Polepaka Sanjeeva^{1*}, G. Praneeth Reddy¹, Vijaylakshmi Sajwan², Bande Ganesh³[8] identified a number of issues with the blockchain voting apps that were already in development and offered an improved solution with strong security, trust, and transparency. This study aims to provide light on some recent developments on the security and privacy concerns related to blockchain-based electronic voting. In conclusion, we have presented a comparative analysis of the security and privacy specifications of the current system.

III. PROPOSED SYSTEM

The proposed system functions similarly to a digital wallet, MetaMask will serve as the intermediary between the user interface and the blockchain network, anyone with a basic understanding of computers can participate in the voting process. Remix IDE is used to compile and deploy the smart contract, and fake ether (ETH) can be obtained from Ganache for testing purposes. Ganache and Remix IDE are two tools for implementing the Ethereum blockchain. Because a diverse group of people will be using the system, the user interface has been built to be as easy as possible so that everyone may use it without difficulty. HTML, CSS and JAVASCRIPT is used in the design of the user interface.

A cryptocurrency wallet program called MetaMask is used to communicate with the Ethereum network. Through a mobile app or browser extension, it enables users to access their Ethereum wallet, which may be used to engage with decentralised applications. ConsenSys Software Inc., a blockchain software business that specialises in Ethereum-based tools and infrastructure, is the developer of MetaMask.

With the help of a suitable web browser or the built-in browser of the mobile app, MetaMask users may safely connect to decentralized services, broadcast transactions, transfer and receive Ethereum-based cryptocurrencies and tokens, save and manage account keys, and more.

Following verification, when the user logs into the system, the MetaMask appears. To access, the user must always enter their password as shown in Figure 1, choose the account they want to vote on, and all voter accounts initially receive ether, which is used for petrol and transaction fees.

Blockchain is a peer-peer network, where there wouldn't be any centralized system which makes it more secured and also blockchain runs on a web3 network in which the user can access their own data and it cannot be sold to third parties.

The results will be computed based on the quantity of transaction through blockchain that the user sends. The contender who finishes with the most votes will be deemed the winner, and the outcome will be made public. The development and implementation of a decentralized e-voting system utilizing blockchain technology have shown promising outcomes. The system was designed to enhance transparency, security, and accessibility in the voting process. Through the utilization of a distributed ledger system, each vote cast by a participant was securely recorded, encrypted, and stored in a transparent and immutable manner.

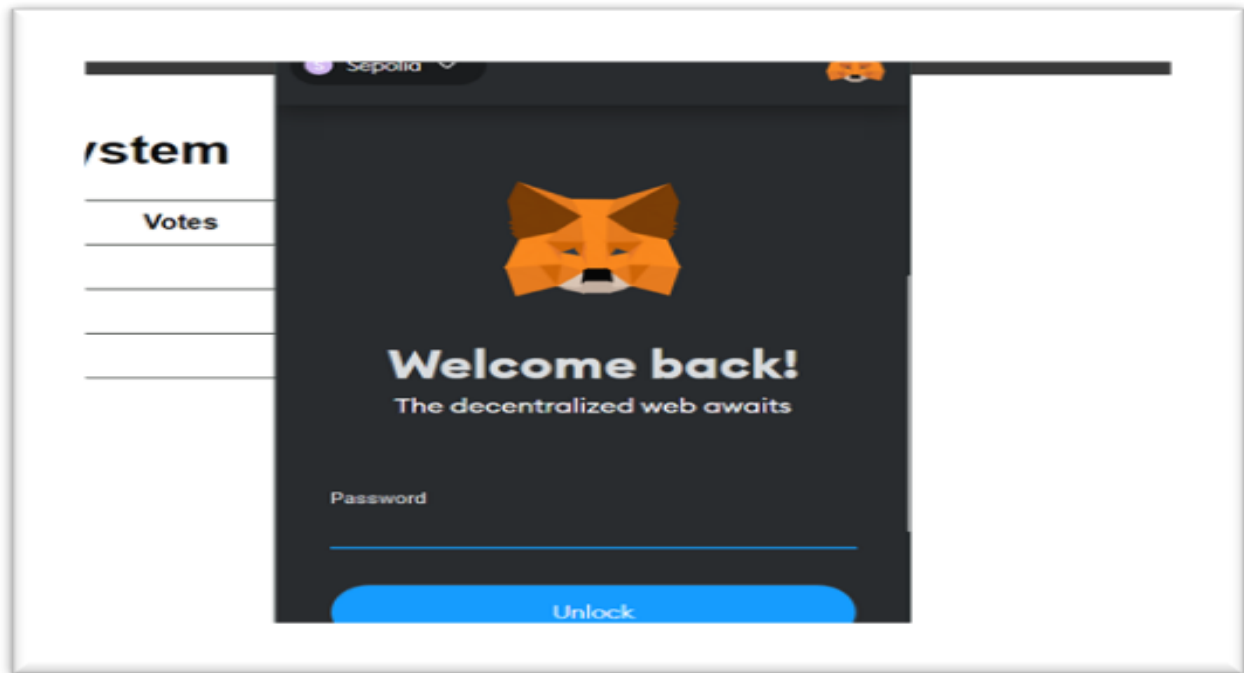


Figure 1 MetaMask Login

One tool that can assist you in better understanding the transactions you do with MetaMask and receiving assistance with them when needed is MetaMask Activity. Any legitimate blockchain address may be looked up, and the transactions linked to that account can be consulted.

The user would be presented with a table where they may cast their vote based on the serial number after successfully connecting to the MetaMask. The MetaMask will reappear after hitting the vote button and request an acknowledgement to verify the transaction [9], as shown in Figure 2.

Through this medium, user can see their transaction history to verify their votes at any time. This improves the verifiability of the system and allows user to cast their vote in a more secured method. The system provides an anonymity where all the details about the user and candidates are stored in the form of hash value (i.e., the 16-digit hexadecimal values), these features make the system really hard to crack and also have false manipulation among voters.

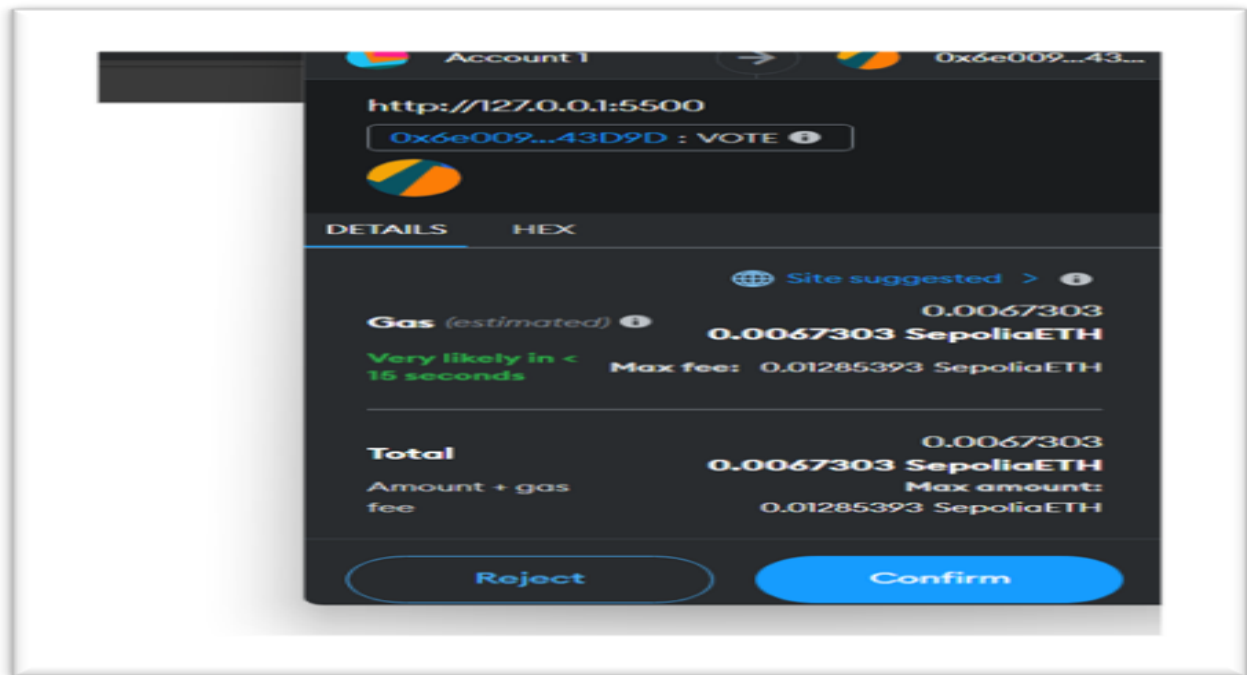


Figure 2 MetaMask Transaction details

The voting page is very straightforward; it consists of a table that contains a list of candidates, and voters can choose a candidate with their corresponding candidate, as seen in Figure 3. Below the table, we can clearly see there is a text box that asks to enter the ID of the candidate to whom the candidate wishes to vote.

Once the candidate selects the Candidate ID and clicks on the vote button, the MetaMask will pop up showing the gas fee and amount for transaction and only if the voter clicks on confirm as shown in the Figure 2.

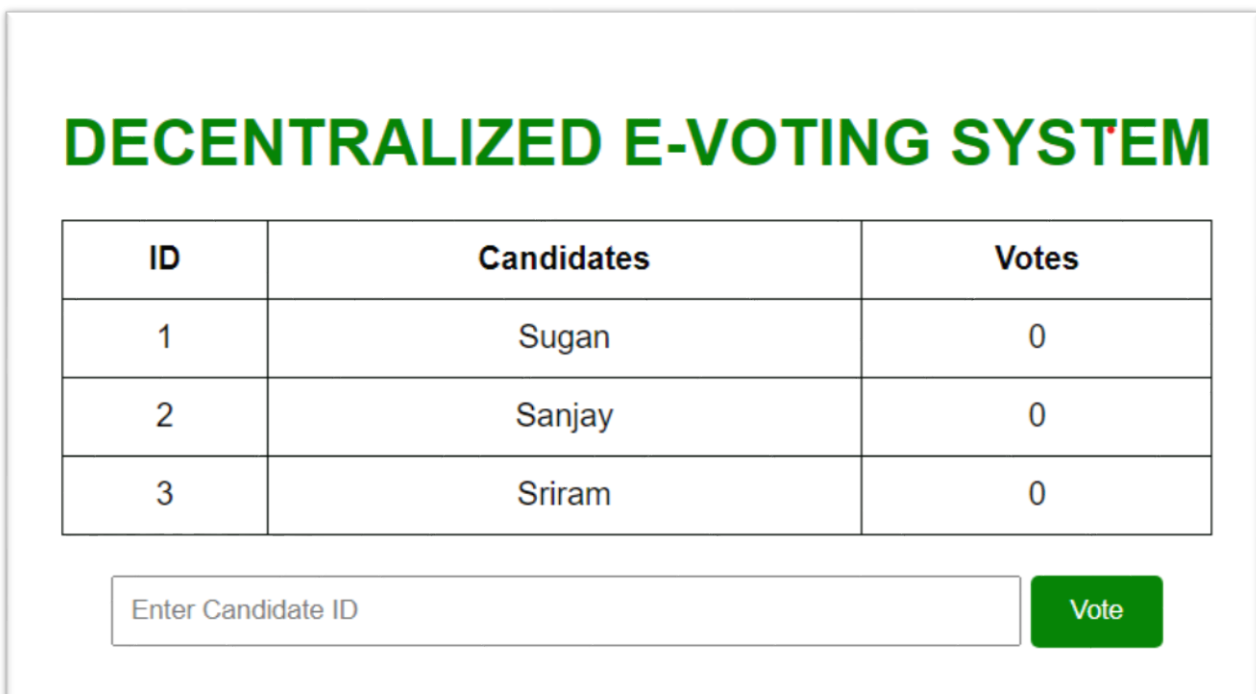


Figure 3 Voting process

The voter can always check the transaction history to confirm their vote, and the table will be updated, as these are the client-side features that allow the user to engage with the system. The smart contract is created, compiled, and deployed in the Remix IDE, where the subsequent steps are completed. The aforementioned numbers 1, 2, and 3 make it quite evident how user-friendly and transparent our Decentralized Voting System interface is.

The Remix IDE is an online development platform that allows users to write, compile, and deploy smart contracts, as depicted in figure 4. It also includes multiple testing IDs that allow users to test deployed contracts. Once a contract is deployed, it generates a deployed address that needs to be added to the JavaScript code in order to connect the client-side, MetaMask, and the smart contract.



Figure 4 Remix IDE

The client-side application and blockchain network comprise the system's overall architecture, as illustrated in Figure 5. MetaMask serves as a mediator between the two components. The client-side application is created using HTML, CSS, and JavaScript, while the blockchain network is made up of smart contracts that are deployed using Remix IDE and written in Solidity.

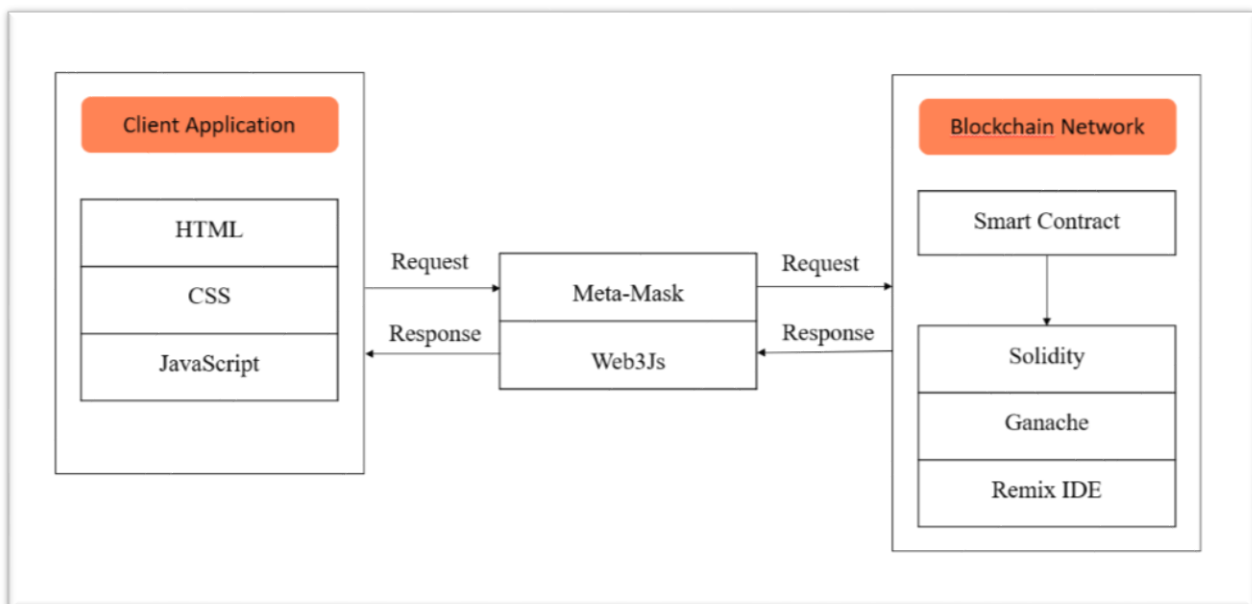


Figure 5 System Architecture

This approach works as follows: when a user logs in, MetaMask [10] appears and requests that they provide their password in order to connect. The twelve key values can also be used by the user to reset their MetaMask password in the event that they forget it. Once the user has connected to the MetaMask, they will be taken to the voting page where they can select a candidate and validate the transaction. Once they have cast a vote, they will only be able to verify it and cannot cast another one. Following a successful vote, they can lock MetaMask and log out of the system, as seen in figure 6.

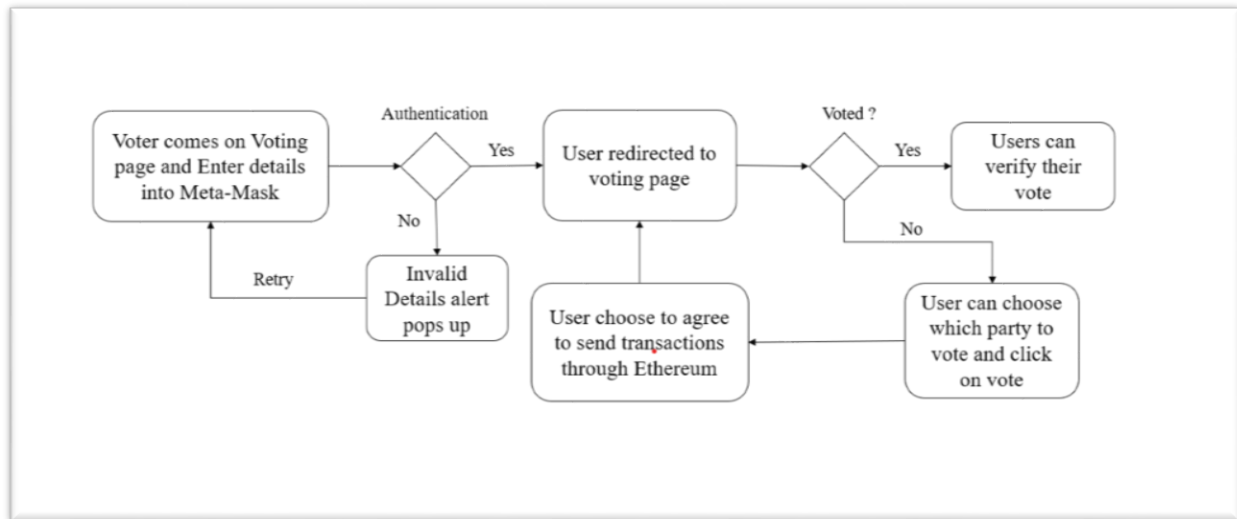


Figure 6 Working Methodology

IV. EVALUATION

The following criteria are to be used in evaluating the suggested system:

- Anonymity
- Security
- Verifiability
- Decentralized
- Authentication
- Integrity
- Privacy

ANONYMITY: Because the 16-digit bit only represents users and votes, voter information such as name and who they have voted for is kept private. No outside party using the system is able to learn about the voters.

SECURITY: The system offers a secure platform for users to cast their ballots because all entered information and votes are unchangeable and extremely difficult or impossible to hack.

VERIFIABILITY: Voters are given the certainty that the correct candidates are receiving their cast ballots. Voters can notice an increase in the candidate's vote total when they cast their ballots, and they can use the MetaMask transaction history to verify the vote at any time the system is available.

DECENTRALIZED: The system as a whole is fully decentralised, meaning that there is no central hub or control system. Any modifications require changing all of the pre-systems, which is extremely difficult, and that changes made to one block do not affect changes made to any other blocks.

AUTHENTICATION: Since the system's first step is to ask for a password to unlock the MetaMask, only authorised users are able to create and provide MetaMask IDs, meaning that only verified users are permitted access to the system.

INTEGRITY: We can categorically state that this system possesses integrity, which is the capacity to withstand alterations of any kind to the data and accuracy of the data during the course of its lifetime.

PRIVACY: Because this system employs asymmetric cryptography, multiple keys are used during transactions, enhancing the security and privacy of user data.

V. CONCLUSION

The primary goal of developing the decentralized blockchain-based electronic voting system was to solve some of the problems with the existing digital voting system. People find it very difficult to travel long distances and stand in line for long periods of time in order to cast their votes. Additionally, there are many who question whether they voted for the correct candidate or whether there was fraud involved in the counting process. These are the problems with the way the voting system is now set up.

The suggested system will solve all of the aforementioned issues with the current one because users won't have to travel far or wait in queue to cast their ballots, and they can always verify who has cast their ballot and when.

Following the successful completion of this suggested work, voting is employed in many places, such as colleges, where there is an elective paper selection process and elections. As a result, this system would have a significant impact on society beyond the election process. Voting procedures are used in the IT industry, as well as in any other industry, from big corporate to small-scale community leader selection.

The trust of users is the most important requirement for any system. Users will undoubtedly have faith in this system since it allows them to monitor all of their activity at any time and establishes restrictions such as transaction confirmation and a single vote per user.

We can therefore conclude that voting fraud can be significantly decreased and the percentage of people who cast ballots can be raised.

REFERENCES

- [1] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam. Digital Voting: A Blockchain-based E-Voting System using Bio-hash and Smart Contract, CFP20P17-ART; ISBN: 978-1-7281-5821-1 (2020).
- [2] Prof. S. S. Adagale, Prajwal Shiwal1, Dhruv Morey2, *; Decentralized E-Voting System Using Blockchain, ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue XII Dec 2022.
- [3] Kriti Patidar, Dr Swapnil Jain, "Decentralized E- Voting Portal Using Blockchain", (2019).
- [4] Uzma Jafar, Mohd Juzaidin Ab Aziz, Zarina Shukur and Hafiz Adnan Hussain, A Systematic Literature Review and Meta-Analysis on Scalable Blockchain Based Electronic Voting Systems (2020).
- [5] Yousif Osman Abuidris, Rajesh Kumar and Wang Wenyong, "A Survey of Blockchain Based on E- voting Systems"
- [6] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Blockchain-Based E-Voting System, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.
- [7] Mayur Shirsath, Mohit Zade, Riteshkumar Talke, Praful Wake and Maya Shelke, "Survey on Voting System using Blockchain Technology" (2019).
- [8] Polepaka Sanjeeva1*, M. Sai Sathwik1, G. Sai Prasad1 G. Praneeth Reddy1, Vijaylakshmi Sajwan2, Bande Ganesh3, "Decentralized and Automated Online Voting System using Blockchain Technology", (2023)
- [9] Naina Nagesh Dhepe and Dr Pathan Mohd Shafi, "A Survey on Smart Electronic Voting System Using Blockchain Technology" (2021)
- [10] Chang-Hyun Roh* and Im-Yeong Lee**. A study on electronic voting system using private blockchain. JOURNAL OF INFORMATION PROCESSING SYSTEMS, (2020)