Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS-2023)
IEEE Xplore Part Number: CFP23K74-ART; ISBN: 979-8-3503-9725-3

2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) | 979-8-3503-9725-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICCS56967.2023.10142546

A Secure and Decentralized Method of E-voting using Blockchain and Smart Contracts

Kirit Enuga [*], Pranay Batthula [*], Sai Shashank Aleti [*], Nitish Kolluru [*], Sakthidharan G. R. [#]

[*]UG Student, Department of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana
[#]Professor, Department of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana
[*]enugak@gmail.com

***Abstract*— Blockchain has already been used in developing many applications, including cryptocurrencies and NFTs. With the help of blockchain and smart contracts, a Decentralized E-Voting System can be developed. A Decentralized E-Voting System is used for activities like voting, verifying the user's details, adding candidates, starting and ending the election, self-tallying the total number of votes, and giving the results of the elections. A system using blockchain is more secure, faster, transparent, and immutable. The existing systems for voting are less secure as they use EVMs and VVPATs, which can be tampered with. The existing systems are also slower than the proposed model in terms of the time taken to announce the results. There are other problems like Vote Rigging, Polling Booth Capture, and Voting Manipulation. With the increasing risk of cyberattacks, it is of utmost importance to have an online voting system capable of withstanding these attacks. A blockchain-based e-voting system will enable user confidentiality using encryption. The platform is created on the Ethereum network that makes use of smart contracts written in the Solidity programming language. Truffle, Ganache and Metamask are the tools used to create a Decentralized E-Voting System.**

Keywords*— Blockchain, Smart Contracts, Decentralized, E-voting, Self-tallying.

I. INTRODUCTION

The adoption of electronic voting systems has been increasing in different parts of the world, with many countries embracing this technology for their national elections. Estonia was the first country to implement an electronic voting system for its national elections, which has inspired other nations to adopt similar systems [1]. Nigeria, Switzerland, and Norway have all adopted electronic voting systems for their state and council elections. However, despite the benefits of electronic voting systems, some traditional electronic systems do not provide anonymity and integrity.

In recent years, many countries have faced different issues with clarity and fairness during the balloting process. In some instances, voters are not sure of their rights or the configuration of leadership. This scenario is prevalent in countries such as Nigeria, India, Brazil, Pakistan, and Bangladesh, where occurrences of fraudulent votes, early voting, casting duplicate ballots, insufficient implementation of laws and audits, political unrest, and inadequate knowledge about the voting process have been reported.

To address these issues, some countries have started to adopt cutting-edge technologies such as blockchain. The use of blockchain technology has gained a significant impact on electronic voting systems. This technology provides anonymity, integrity, and transparency, which are essential for a fair and reliable voting system.

For instance, countries such as South Korea, Russia, and Switzerland have implemented blockchain-based voting systems for their national elections. In South Korea, the government implemented a blockchain voting system for citizens living overseas, while Russia and Switzerland are currently testing blockchain voting systems for their national elections.

Blockchain technology has the potential to revolutionize the way elections are conducted, ensuring that the voting process is transparent, secure, and efficient. However, as with any new technology, there are concerns about its implementation and possible vulnerabilities. Therefore, governments need to ensure that the blockchain-based voting system is secure and that all stakeholders have trust in the technology.

Decentralized voting systems that use blockchain technology can achieve stability by leveraging smart contracts. These contracts are self-executing computer programmes designed to run automatically when certain conditions are met. They are securely stored on the blockchain. Elections may make use of smart contracts to ensure that procedures are followed and that every vote is appropriately counted. The agreements might be made to ensure the validity of each vote, prevent fraud like double voting, and preserve the election's regulations [2]. As a result, the systembecomes transparent and dependable.

An e-voting system that is decentralized and based on blockchain technology and smart contracts would use a distributed ledger, where every voter would possess a distinct digital identity, and the votes would be registered as transactions. These transactions would be combined into blocks, and each block would be connected to the preceding block, forming a chain of blocks, or a blockchain [3].

Once the voter is identified and authenticated, the voter can cast their vote by creating a transaction on the blockchain. The smart contract would then validate the vote, making sure that the voter is eligible, that the voter has not voted before, and that the vote is in the correct format. Once the vote is validated, it would be recorded on the blockchain, where it would be visible to everyone, but tamper-proof.

The smart contract would also control the vote-counting process. The smart contract would be programmed to only count the valid votes, and it would be able to automatically calculate the results. The transparency and immutability of the blockchain would ensure that the vote-counting process is accurate and tamper-proof [4].

One of the most significant advantages of this system is that it is based on transparency and the immutability of blockchain technology, which is considered a key feature to prevent vote manipulation, hacking, or other forms of fraud.

There are several reasons why a decentralized e-voting system using smart contracts and blockchain technology is needed.

- Security: Traditional electronic voting systems are vulnerable to hacking, manipulation, and other forms of fraud. A decentralized e-voting system using blockchain technology would provide a more secure voting process, as it would be virtually impossible to hack or manipulate the results.

- Transparency: The use of blockchain technology would provide a permanent and unchangeable record of the vote, which would make the vote-counting process transparent and tamper-proof. This would increase the public's trust in the voting process.

- Accessibility: With a decentralized e-voting system, voters would be able to cast their vote from anywhere, at any time, as long as they have an internet connection. This would increase voter turnout and make the voting process more convenient for voters.

- Cost-effective: The use of blockchain technology would eliminate the need for a central authority to oversee the voting process, which would reduce the overall costs of the voting process [5].

- Identity verification: Blockchain technology allows for secure and decentralized identity verification, which would make it easier to verify a voter's identity and prevent voter fraud [6].

II. Related Work

"A Blockchain-based Decentralized Voting System" by T. M. Muthukumar and V. M. Mohan Kumar proposes a decentralized voting system using blockchain technology, which aims to improve the transparency and security of the voting process. The authors discuss the architecture of the proposed system, as well as its implementation and evaluation [7].

"A Survey on Blockchain-based Voting System" by N. M. Hemalatha and M. Nithya provides an overview of blockchain-based voting systems and discusses the benefits and challenges of using blockchain technology for elections. The authors also survey the existing literature on blockchain-based voting systems and highlight some of the most promising approaches [8].

"E-Voting Based on Blockchain: The Case Study of Moscow City Duma Elections" by A. V. Kuleshov, V. G. Kurbatskiy, and A. V. Shorov describes the blockchain-based voting system that was used in the Moscow City Duma elections in 2019. The authors discuss the design and implementation of the system, as well as its evaluation and lessons learned [9].

"Blockchain Voting: A Comprehensive Guide" by Coinmonks provides an overview of blockchain-based voting systems and discusses the benefits and challenges of using blockchain technology for elections. The authors also survey some of the existing blockchain-based voting platforms, including Voatz and Agora [10].

"Blockchain Voting Systems: A Survey" by F. Roshan, M. T. Hossain, and M. Hasan surveys the existing literature on blockchain-based voting systems and provides a comprehensive overview of the benefits and challenges of using blockchain technology for elections. The authors also discuss some of the most promising approaches to building blockchain-based voting systems [11].

III. Existing Systems

A. Paper Ballots

A ballot paper is a physical or digital document used in voting to record the preferences of voters. The document contains the names of candidates and voters mark their preferred choices on the document. The ballots are collected and counted to determine the outcome of an election or referendum.

While ballot papers have been used for centuries, they have certain limitations that can compromise the integrity of the voting process. For example, ballot papers can be tampered with or lost, leading to inaccurate vote counts. Additionally, the manual counting process can be time-consuming and error-prone.

B. EVMs

Electronic Voting Machines (EVMs) are computer-based devices that have been developed to facilitate secure and efficient voting in elections. EVMs have become increasingly popular in recent years due to their ability to eliminate the problems associated with traditional paper-based voting systems, such as ballot stuffing, invalid ballots, and time-consuming vote counting. However, EVMs are not without their own set of issues and challenges.

One of the main issues with EVMs is the potential for tampering and hacking. Because EVMs rely on computer software and hardware to function, they are vulnerable to attacks by hackers and malicious actors who may seek to alter the election results or compromise the integrity of the voting process. This is particularly concerning in countries where election results can have significant consequences for the political landscape and the future of the country.

Another issue with EVMs is the lack of transparency in the voting process. Traditional paper-based voting systems allow voters to physically mark their ballots and see them being placed in a ballot box. This provides a level of transparency and accountability that is not present in EVMs, where the voting process is entirely electronic and difficult to verify. This can lead to a lack of trust in the voting process and raise concerns about the accuracy of the election results.

EVMs can also be prone to technical malfunctions and errors. For example, EVMs may experience glitches or software bugs that can lead to inaccurate vote counts or even cause the machine to crash. This can lead to delays in the voting process and undermine confidence in the accuracy of the results.

EVMs can also present accessibility challenges for certain groups of voters, such as those with disabilities or limited technological literacy. These voters may struggle to use the EVMs effectively, which can lead to voter disenfranchisement and undermine the principles of fairness and equality in the voting process.

IV. Proposed System

Imagine a chain made up of individual blocks to quickly grasp the idea of a blockchain. These blocks include an enormous quantity of data that is gathered and processed via a process known as mining. Each block is given a distinct digital fingerprint, or hash, to ensure the chain's security. Every block also contains a reference to the block before it, creating a linked list structure that dates back to the Genesis Block, the very first block ever made. A blockchain is made by connecting each block to the one before it, creating a transparent and unaltered record of all the data contained therein [12].

Ensuring the security of the blockchain is crucial to developing a reliable decentralized voting system. To achieve this, several measures must be implemented, such as the use of advanced cryptographic algorithms to protect the data and prevent tampering. The system should also include a secure method for identifying and authenticating voters to prevent fraudulent activities. Additionally, the blockchain network should be distributed across multiple nodes to prevent a single point of failure, and regular backups of the blockchain should be maintained to prevent data loss. A secure and reliable network infrastructure with proper firewall and access control should also be established to prevent unauthorized access to the system. Finally, to find and address possible security holes in the system, routine security audits and vulnerability assessments should be conducted. By putting these precautions in place, a trustworthy and secure blockchain-based voting system may be created to guarantee the validity of the voting procedure [13].

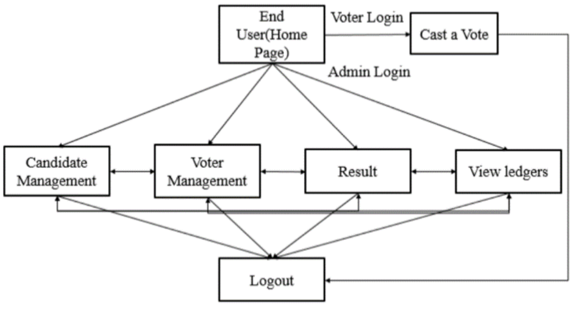


Fig. 1 Architecture of the system

A. Algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a widely used cryptographic hash function that is used to ensure the security and integrity of data in various applications, including blockchain technology.

In the context of blockchain-based voting systems, SHA-256 is used to create a unique digital fingerprint or hash for each block that is added to the blockchain. This hash is generated by inputting the data contained in the block (such as the voting records) into the SHA-256 algorithm, which then produces a fixed-length hash value. This hash value is unique to the specific data input and cannot be reversed to retrieve the original data, making it a secure and tamper-proof way to store voting records.

One advantage of using SHA-256 in blockchain-based voting systems is that it ensures the accuracy and immutability of the voting records. Once a block has been added to the blockchain, the data contained within it cannot be altered without changing the hash value of the block, which would require a significant amount of computing power and time. This makes it difficult for malicious actors to tamper with the voting records, ensuring the security and integrity of the voting process.

SHA-256 is widely recognized and trusted as a secure cryptographic hash function that has been thoroughly tested and evaluated for security. It is part of the SHA-2 family of algorithms, which is a US government standard for secure hash functions. This standardization and widespread adoption make it a more reliable and secure solution for blockchain technology compared to other encryption algorithms that may not have undergone the same level of scrutiny and evaluation.

Additionally, SHA-256 is computationally efficient, which is essential for blockchain technology to handle a large volume of transactions while maintaining security and integrity. It is capable of generating a fixed-length hash value for any input data, making it a reliable and consistent solution for blockchain applications.

B. Reliability

Reliability is a critical aspect of any voting system, and it becomes even more important in a decentralized voting system using blockchain technology. In such a system, reliability is achieved by ensuring that the votes are accurately recorded and counted while maintaining the integrity and security of the voting process.

By using smart contracts, decentralised voting systems that employ blockchain technology can achieve stability. These contracts are self-executing computer programmes that are safely kept on the blockchain and are made to run automatically when specific requirements are satisfied. Smart contracts may be used in elections to guarantee that rules are followed and that every vote is correctly tallied. The contracts may be set up to verify the legitimacy of each vote, thwart any fraud like multiple voting, and uphold the rules of the voting process. The system thus gains dependability and transparency.

Another way reliability is achieved is through the use of consensus algorithms. Consensus algorithms ensure that all nodes in the blockchain network agree on the state of the blockchain, including the voting records. This agreement is critical in ensuring that the voting process is reliable and that the votes are accurately recorded and counted. Consensus algorithms such as Proof-of-Work or Proof-of-Stake require network participants to solve complex mathematical problems or stake a certain amount of cryptocurrency to validate transactions and create new blocks. These algorithms ensure that the network is secure and trustworthy, making it a reliable solution for decentralized voting systems.

C. Design Details

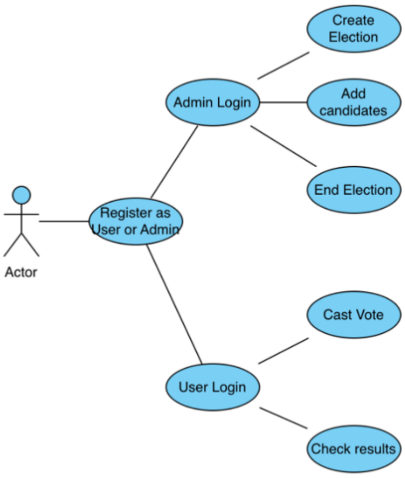
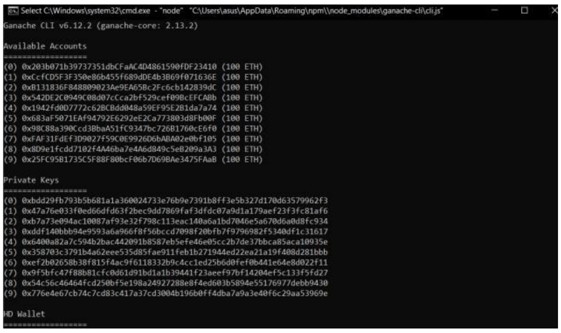


Fig. 2 Use case diagram

1) Smart Contracts: In Solidity, a smart contract is a programme that executes on the Ethereum blockchain and can carry out certain tasks automatically following predetermined guidelines and criteria. A contract-oriented programming language created exclusively for the Ethereum blockchain is called Solidity. The contract interface and the contract implementation are the two main components of a smart contract in Solidity. While the contract implementation specifies the logic and rules that govern those functions, the contract interface specifies the functions that may be invoked by outside users.

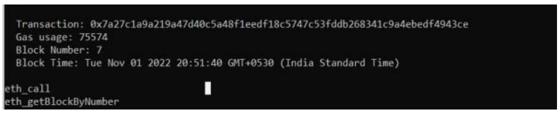
2) Ganache: Once we are done with the smart contracts, we will move on to the next step. The next step involves running the local Ethereum Network by using the ganache-cli command. Ganache is an Ethereum environment. It is used for developing, testing, and deploying the application. Ganache is available as a CLI(Command Line Interface) and a UI(User Interface). In the project, we will be using the CLI. The ganache-cli command needs to be running at all times. The ganache-cli command generates 10 accounts along with 10 private keys.



```
Select C:\Windows\system32\cmd.exe - "node"  "C:\Users\asus\AppData\Roaming\npm\\node_modules\ganache-cli\cli.js"
Ganache CLI v6.12.2 (ganache-core: 2.13.2)

Available Accounts
==================
(0) 0x203b071b39737351dbCFaAC4D4861590fDF23410 (100 ETH)
(1) 0xCcfCD5F3F350e86b455f689dDE4b3B69f071636E (100 ETH)
(2) 0xB131836F848809023Ae9EA65Bc2Fc6cb142839dC (100 ETH)
(3) 0x542DE2C0949C08d07cCca2bf529cef09BcEFCA8b (100 ETH)
(4) 0x1942fd0D7772c62BCBdd048a59EF95E2B1da7a74 (100 ETH)
(5) 0x683aF5071EAf94792E6292eE2Ca773803d8Fb00F (100 ETH)
(6) 0x98C88a390Ccd3BbaA51fC9347bc726B1760cE6f0 (100 ETH)
(7) 0xFAF31FdEf3D9027f59C0E9926D6bABA02e0bf105 (100 ETH)
(8) 0x8D9e1fcdd7102f4A46ba7e4A6d849c5eB209a3A3 (100 ETH)
(9) 0x25FC95B1735C5F88F80bcF06b7D69BAe3475FAaB (100 ETH)

Private Keys
==================
(0) 0xbdd29fb793b5b681a1a360024733e76b9e7391b8ff3e5b327d170d63579962f3
(1) 0x47a76e033f0ed66dfd63f2bec9dd7869faf3dfdc07a9d1a179aef23f3fc81af6
(2) 0xb7a73e094ac10087af93e32f798c113eac140a6a1bd7046e5a670d6a0d8fc934
(3) 0xddf140bbb94e9593a6a966f8f56bccd7098f20bfb7f9796982f5340df1c31617
(4) 0x6400a82a7c594b2bac442091b8587eb5efe46e05cc2b7de37bbca85aca10935e
(5) 0x358703c3791b4a62eee535d85fae911feb1b271944ed22ea21a19f408d281bbb
(6) 0xef2b02658b38f815f4ac9f6118332b9c4cc1ed25b6d0fef0b441e64e8d022f11
(7) 0x9f5bfc47f88b81cfc0d61d91bd1a1b39441f23aeef97bf14204ef5c133f5fd27
(8) 0x54c56c46464fcd250bf5e198a24927288e8f4ed603b5894e55176977debb9430
(9) 0x776e4e67cb74c7cd83c417a37cd3004b196b0ff4dba7a9a3e40f6c29aa53969e

HD Wallet
==================
```

Fig. 3 Ganache-generated accounts along with the public keys

3) Gas: In the Ethereum network, "gas" refers to the unit of measurement for computational work required to execute a certain operation on the network. Gas is required to pay for the computational work done by the Ethereum network's nodes, such as validating transactions and executing smart contracts. When a user wants to perform a certain action on the Ethereum network, such as sending a transaction or executing a smart contract, they must pay for the gas required to perform that action. The gas is paid in Ether (ETH), which is the native cryptocurrency of the Ethereum network. The cost of gas is determined by the current market price of Ether and the current gas price. The more complex the operation, the more gas it will require. For example, a simple transaction like sending Ether from one address to another will require less gas than a more complex operation like executing a smart contract.



```
  Transaction: 0x7a27c1a9a219a47d40c5a48f1eedf18c5747c53fddb268341c9a4ebedf4943ce
  Gas usage: 75574
  Block Number: 7
  Block Time: Tue Nov 01 2022 20:51:40 GMT+0530 (India Standard Time)

eth_call
eth_getBlockByNumber
```

Fig. 4 A block generated at the end of a transaction.

4) Metamask: Metamask is an online cryptocurrency wallet. It is used for interacting with the Ethereum blockchain. It can be accessed as an extension through a browser on a computer or mobile phone. Metamask is used for storing the wallets generated using the ganache-cli command. This is done by linking the wallets we created earlier to Metamask. The linking is done by choosing a key from Ganache and importing the wallet on Metamask using the private keys. Each account will contain 100 ETH upon its creation. Once the users start interacting with the site, small amounts of this currency are deducted from their wallets. This deduction is better known as gas. Gas is the fee that is deducted for performing the computational effort.

5) NodeJS Server: Node.js allows developers to use JavaScript to write server-side code, which can be used to create web applications, APIs, and other types of back-end systems. Node.js provides a built-in runtime environment that allows developers to execute JavaScript code without the need for a browser. This allows developers to use a single language (JavaScript) for both the front-end and back-end of their applications, which can make development faster and more efficient.

D. Procedure

The proposed decentralized voting system is built using Ganache, Truffle, MetaMask and Node.js. It uses the Ethereum blockchain to create a secure and transparent voting system that can be used for any type of election.

The system comprises of a smart contract that is deployed on the Ethereum blockchain and that automates the voting process. The smart contract is responsible for verifying and counting the votes, and it is accessible to all the voters who can interact with it and cast their votes.

The digital identity management system is used to create and verify digital identities for the voters. This can be done using a self-sovereign identity system or a centralized identity verification system.

The voter interface is the interface that voters use to interact with the system, such as a web application or a mobile app. The interface allows the voters to cast their votes, view the results, and check the status of their votes.

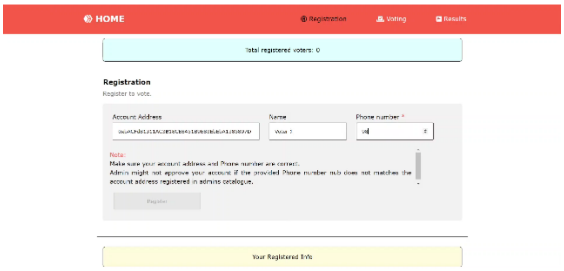
A Node.js server is used to interact with the Ethereum blockchain through Metamask and the smart contract. This server will be responsible for handling voters' requests, validating the votes, and sending the vote to the smart contract.

A browser plugin called Metamask enables users to communicate with the Ethereum blockchain, the smart contract, and the Node.js server. It may also be used to generate voter digital identities. Access restrictions and encryption are used to safeguard the system, making sure that only authorised people can use it and that the data is shielded from prying eyes.

Before deployment, the system is carefully tested, and any defects or problems are resolved. The system is set up and made accessible to users on a live blockchain network, such as the mainnet of Ethereum.

V. RESULTS

The proposed model is created using smart contracts written in Solidity, and Ganache for testing, deploying and developing, Metamask to interact with the server and Node.js to interact with the Ethereum blockchain. The figure given below shows the voter registration page. The voter will have to enter his name and phone number.



Total registered voters: 0

Registration

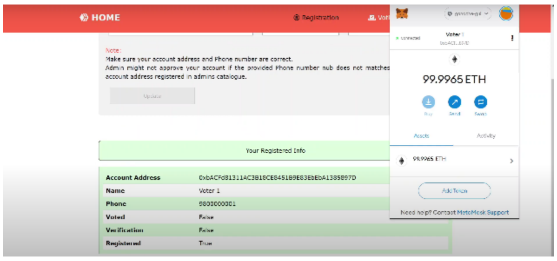
Register to vote.

Account Address: 0xbACFd81311AC3B18CE8451B9E83EbEbA1385897D
Name: Voter 1
Phone number *: 98

Note:
Make sure your account address and Phone number are correct.
Admin might not approve your account if the provided Phone number nub does not matches the account address registered in admins catalogue.

Fig. 5 Voter Registration Page.

The figure given below shows the details of the registered user. The details include account address, name, phone number, and whether the voter has voted or not.



Note:
Make sure your account address and Phone number are correct.
Admin might not approve your account if the provided Phone number nub does not matches the account address registered in admins catalogue.

Account Address	0xbACFd81311AC3B18CE8451B9E83EbEbA1385897D
Name	Voter 1
Phone	9800000001
Voted	False
Verification	False
Registered	True

Voter 1

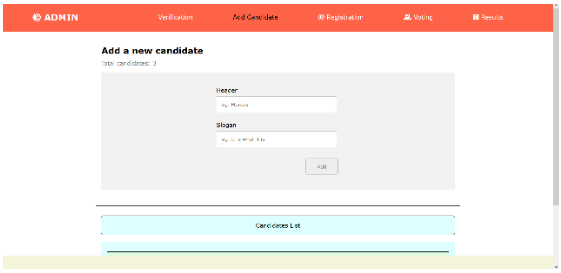
99.9965 ETH

99.9965 ETH

Need help? Contact MetaMask Support

Fig. 6 Voter's Registered Information

The figure given below is used for adding candidates to the election. The administrator will be able to add the candidates along with the slogan.



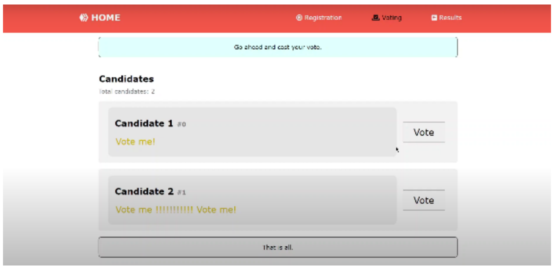
Add a new candidate

Total candidates: 3

Header: eg. Marcus
Slogan: [illegible]

Fig. 7 Candidate addition page

The figure given below shows the voting page for the voters. A voter will be able to vote for one candidate from the list of candidates.



Go ahead and cast your vote.

Candidates

Total candidates: 2

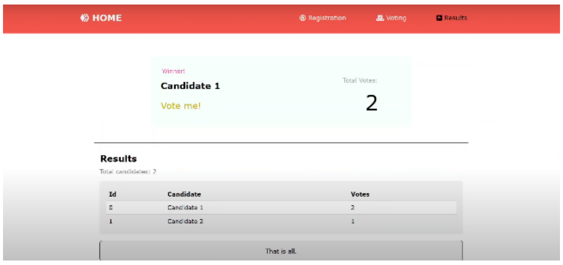
Candidate 1 #0
Vote me!

Candidate 2 #1
Vote me !!!!!!!!!!! Vote me!

That is all.

Fig. 8 Voting Page for the users

The figure given below shows the results of the election. The winner of the election is displayed upon completion of the election along with the total number of votes obtained.



Winner!
Candidate 1
Vote me!
Total Votes:
2

Results

Total candidates: 2

Id	Candidate	Votes
0	Candidate 1	2
1	Candidate 2	1

That is all.

Fig. 9 Results of the election

VI. CONCLUSIONS AND FUTURE SCOPE

This article presents a novel decentralized voting platform that leverages the Ethereum blockchain technology. The platform's key feature is its ability to prevent multiple votes per user, ensuring the voting process's integrity and fairness.

Furthermore, the proposed platform can be enhanced to make it suitable for national government elections by incorporating fingerprints or other devices located at voting centres. The user interface and results visualization can be customized to meet the specific requirements of the customer, ensuring a tailored and optimal user experience.

The decentralized voting platform has the potential to replace centralized voting systems, making it applicable for various types of elections, including government elections, competitions, and expositions, among others. Additionally, the platform offers new opportunities for voting service providers, who can work with voting event organizers and voters.

The voting service provider can deploy the voting smart contract on the Ethereum network and earn revenue from both the voting event organizers and voters upon registration and voting. The platform's flexibility and potential for revenue generation make it an attractive solution for various voting needs.

The vote-counting process has been designed to eliminate the possibility of a single point of failure, as each ballot is kept separate from others during the counting process. We respect the choice of voters who do not wish to cast ballots and do not believe in pressuring or coercing them into doing so by imposing additional deposits. Furthermore, we can efficiently count thousands of ballots by leveraging the benefits of parallelization to accelerate the vote-counting process.

In conclusion, the proposed decentralized voting platform is a secure, efficient, and customizable solution that can revolutionize the voting process. Its potential to prevent multiple votes, accommodate national government elections, -and offer new revenue opportunities for voting service providers makes it a viable and attractive solution for various voting needs. It also overcomes the issues of centralized voting systems.

ACKNOWLEDGEMENT

This research has been conducted under the supervision of faculty and aid from the Gokaraju Rangaraju Institute for Engineering and Technology staff.

REFERENCES

[1] Meelis Kitsing, "Internet Voting in Estonia," *GOSE '14 Proceedings of the 2014 Conference on Electro,* 2014.

[2] Fran Casino, Thomas K Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification, and open issues," *Telematics and informatics 36, 55-81,* 2019.

[3] A Shah, Nishita Sodhia, Shruti Saha, "Blockchain-enabled Online-Voting System," *ITM Web of Conferences 32, 03018,* 2020.

[4] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Huaimin Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services 14(4), 352-375,* 2018.

[5] Joe Abou Jaoude, Raafat George Saade, "Blockchain applications-usage in different domains," *IEEE Access 7, 4536045381,* 2019.

[6] Jordi Puiggali, Jordi Cucurall, Robert Krimmer, Sandra Guasch, "Verifiability experiences in government online voting systems," *International Joint Conference on Electronic Voting, 248-263,* 2017.

[7] T. M. Muthukumar. V. M. Mohan Kumar "A Blockchain-based Decentralized Voting System,", 2019.

[8] N. M. Hemalatha, M. Nithya, "A Survey on Blockchain-based Voting System", *International Journal of Advanced Science and Technology, 11416-11421,* 2020.

[9] A. V. Kuleshov, V. G. Kurbatskiy, A. V. Shorov, "E-Voting Based on Blockchain: The Case Study of Moscow City Duma Elections", *International Conference on Computational Science and Its Applications (ICCSA),* 2020.

[10] Blockchain Voting: A Comprehensive Guide https://medium.com/coinmonks/blockchain-voting-a-comprehensive-guide-eca1d4cd202b

[11] F. Roshan, M. T. Hossain, and M. Hasan, "Blockchain Voting Systems: A Survey", *IEEE 7th International Conference on Future Internet of Things and Cloud (FiCloud),* 2019.

[12] Nakamoto, S., "Bitcoin: a peer-to-peer electronic cash system.," 2008.

[13] Umut Can Çabuk, Eylül Adıgüzel, Enis Karaarslan, "A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems," *International Journal of Advanced Research in Computer and Communication Engineering,* 2019.

[14] Gautam Srivastava, Ashutosh Dhar Dwivedi and Rajani Singh, "Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology." *International Conference on Security and Cryptography,* January 2018.

[15] Aggelos Kiayias and Moti Yung, "Self-tallying elections and perfect ballot secrecy," *Lecture Notes in Computer Science, vol. 2274, pp. 141-158,* 2002.

[16] Zhichao Zhao and T.-H. Hubert Chan, "How to vote privately using bitcoin,", *Information and Communications Security, pp. 82-96,* 2016.

[17] Bin Yu, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, et al., "Platform-independent secure blockchain-based voting system", *Information Security: 21st International Conference, pp. 369,* 2018.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", *Ethereum Project Yellow Paper, vol. 151, pp. 1-32,* 2014.

[19] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", *IEEE Access, vol. 4, pp. 2292-2303,* 2016.

[20] Szabó Dániel Attila, "Impact of Social Media on Cryptocurrency Trading with Deep Learning" *Szabó Dániel Attila,* October 26, 2017.

[21] Xuechao Yang, Xun Yi, Fengling Han, "Decentralized Voting: a self-tallying voting system using a smart contract on the Ethereum blockchain," *LNISA, volume, 11233,* 2018.

[22] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Yellow Paper, pp. 1–32,* 2014.