International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

Implementation of Decentralized Blockchain E-voting

Mehul Bafna[1] Abhinay Rajurkar[2] Vedansh Kumar[3] Samir Khan[4] and Prof. Amruta Sankhe[5]
Information Technology, Atharva College of Engineering,Mumbai,India

***Abstract*—This paper proposes a solution to the drawbacks of traditional e-voting Blockchain technology. E-voting is more cost-effective and convenient than the traditional pen and paper method, but it is considered unreliable due to the possibility of physical tampering and a lack of security for voters. By using decentralized Blockchain technology, this research aims to create an e-voting system that guarantees protection of voter identity, secure data transfer, and verifiable results through an open and transparent voting process.**

I. INTRODUCTION

Elections are the process by which voters choose a candidate to hold a public office or official position, thereby establishing a government in a democratic society. Elections have a long history, dating back to ancient Greece, Rome, and the medieval period for selecting popes and emperors, and in India to the Vedic period where rulers were elected by the people. Modern day elections, which began in Europe and North America in the 16th century, have evolved with the use of electronic voting machines (EVMs) replacing the traditional, tedious method. The use of technology in voting has improved efficiency, reduced human error and effort, and increased reliability and accuracy. The proposed system utilizes e-voting, blockchain, and smart contracts for added security and convenience.

A. *E-Voting*

E-voting involves using electronic systems to cast and count votes. The votes are recorded on tape cartridges, diskettes, smart cards, and then sent to a central location for compilation. There are various forms of e-voting, including Direct Electronic Recording (DER) touch screens and optical scanners. The two main types of e-voting are on-site, where electronic voting machines are placed at polling booths and people must physically be there to vote, and remote, where individuals can vote from any location via the internet, SMS, or kiosks. Despite its convenience, the security community views e-voting as unreliable due to security concerns, as the software can be compromised if the device is physically accessed, leading to altered votes. To maintain the integrity of elections, it is important to ensure voters' privacy and protection, while also ensuring a quick and efficient vote counting process

B. *Blockchain*

The conventional approach has been disrupted by the introduction of blockchain, which offers unalterable and transparent systems. Blockchain is a structured data system made up of interconnected blocks. The first block is referred to as the genesis block, and each new block is added to the chain. Each block contains data, a hash, and the hash of the previous block. If any changes are made to a block's data, the hash of that block will change, invalidating not only the altered block but all blocks that come after it. This is to prevent tampering. How- ever, with the advancement of technology, hackers can now compute thousands of hashes in a matter of seconds, making it difficult to prevent tampering. To address this, blockchain uses the proof-of-work concept to slow down the formation of new blocks. Additionally, it operates on a decentralized, peer- to-peer network, where there is no central entity. When a new block is created, it is sent to all other nodes on the network, where each node verifies it for tampering before adding it to their blockchain. All nodes on the network reach a consensus on the validity of the block, making blockchain secure, safe, and reliable

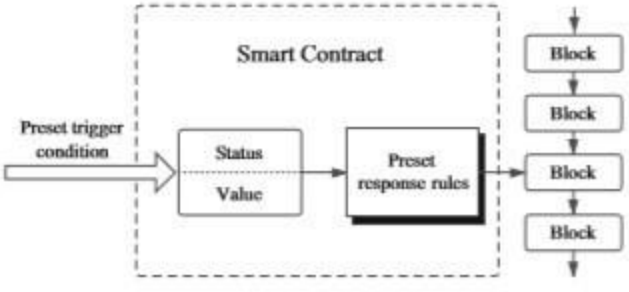

Fig. 1. Working of Smart Contract

C. *Smart Contract*

A smart contract is a type of contract that is automatically enforced using computer code embedded in a blockchain. The code includes a set of rules that govern the interactions and decisions related to the contract between parties. Once the predetermined rules are satisfied, the contract is automatically executed. Smart contracts provide an efficient method of control between two or more parties for the management and distribution of tokenized assets and rights. Fig 1 [1]; shows the working principle of smart contract. Blockchain is a tamper-proof database that is enhanced and empowered by smart contracts

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

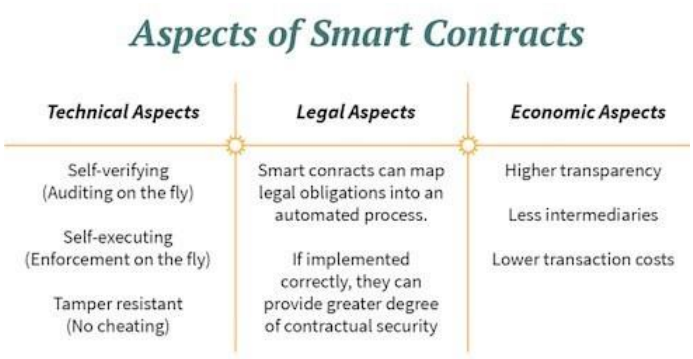

Fig. 2. Diffrent Aspects of Smart Contract

Smart contracts have various facets, including technical legal, and economic perspectives, as depicted in Figure 2[2]

Smart contracts are self-executing agreements between parties whose conditions are encoded into the code. The data interpretation process within the contract ensures its self-verification, and each network node guarantees its proper execution, freeing contract creators from monitoring the contract's execution. Triggers, such as an expiration date, can automatically initiate the contract's execution. In this study, we present a blockchain-based e-voting system designed to address issues in traditional e-voting and promote trust among voters. Our work also serves as a step towards the development of smart governance. The paper is structured as follows: Section 2 reviews prior work in blockchain technology and e-voting systems, Section 3 outlines the proposed blockchain- based e-voting system, Section 4 provides implementation details and results, and Section 5 concludes the study.

II. Related Work

The e-voting system marked a significant improvement over the traditional pen and paper method and gained widespread adoption in many countries. Despite its numerous benefits, including increased voter participation, audibility, affordability, accessibility, and convenience, the e-voting system still faced numerous challenges and problems.

In their study, Abdelwehab et al. [3] highlighted several challenges in the e-voting system, including legal, social and cultural, technical, and security challenges.

Diego F. Aranha et al. [4] conducted an experiment aimed at verifying election results and enhancing transparency and voter participation in electronic elections. Their proposal consisted of two elements: distributed collection of poll tapes using mobile devices by voters and crowdsourcing of election data verification by the electoral authority.

Kristian Gjosteen and Anders Smedstuen [5] had trust in that if voters correctly follow the voting protocol, there would be no risk of attack on the election results and provided a statistical method to improve e-voting security.

Budurudhi et al. [6] analyzed how to design voting machine interfaces to enhance the roles of electors and electoral administrators and applied them to complex elections. The issueof relying on a remote voting device is closely linked to the provided interface, which impacts voting and verification, as important elements in e-voting. Much of the work in remote-electronic voting centres around cryptography-based voting protocol design and verification to maintain desired properties.

Neumann et al. [7] introduced a model for comparing voting schemes in a specific electoral context, applied to the Estonian internet voting scenario.

With various problems arising in electronic voting, especially regarding physical security, blockchain entered the field of e-voting. Ahmed Ben Ayed [8] discussed the utilization of blockchain technology to make e-voting safe, secure, and anonymous. Jen-Ho Hsiao et al. [9] used smart contracts in decentralized blockchain technology for e-voting to involve all voters in evaluating and recording ballots, increasing trust and decreasing the misuse of election capital. Jonathan Alexander et al. [10] utilized NetVote for the user interface of their program, a decentralized application. The dApp admin aids electoral administrators in determining electoral policy, generating voting rules, and opening and closing voting. Voter identification is done through other applications such as biometric readers. TallydApp is used to test and verify election results. This NetVote system is applied to three types of elections: private election, open election, and token holder elections. The current e-voting system is plagued by numerous issues that hinder accurate results, including:

a. Vulnerability to hacking
b. Ineffective auditing
c. Misinterpretation of voter choice
d. Political bias by the manufacturer
e. Tampering with software
f. Inadequate protection of cast votes
g. Hardware failures, etc.

The objective of this study is to design a blockchain- based e-voting system that tackles the persistent challenges posed by legislation. This system can be utilized in various settings, ranging from schools and colleges to office elections and even national-level voting. Our model addresses issues such as vote tampering, machine infiltration, misinformation campaigns and other forms of electoral fraud

III. Proposed System

The proposed system employs several tools, including Ganache, the Truffle framework, NPM, and Metamask. Truffle facilitates the import of smart contracts onto the blockchain, while Ganache manages the internal blockchain and is accessible via Metamask. Users need to have an account to take part with a wallet address and possess Ethereum's cryptocurrency, Ether. To record the transaction on the blockchain, the user must pay a transaction fee, known as gas. Every action and event uses transaction fee to validate the completion of an action (casting a vote, validating the voter/user, etc.)

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

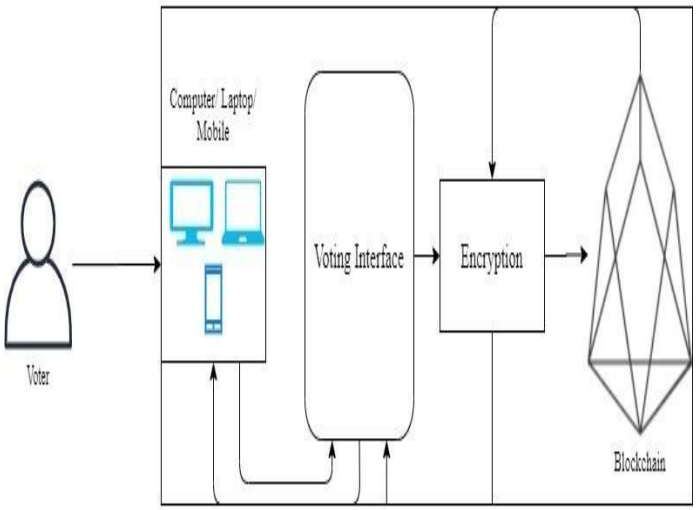

Fig. 3. Proposed E-Voting System Based on Blockchain

A. Preliminaries

Our proposed model requires a 64-bit machine running Windows 7 or later, with NMP dependencies, Truffle framework, Metamask, Solidity toolkit, and Ganache to be installed.

1. Dependency NPM(Node Package Manager)
2. Truffle framework
3. Ganache
4. Metamask
5. Coding language; Solidity, HTML, JavaScript, CSS

NPM (Node Package Manager): NPM (Node Package Manager) is a tool that manages the installation, updating, and removal of Node.js packages in an application. It uses a command-line interface. NPM operates in two modes: local mode, which affects only a specific directory of an application, and global mode, which affects all Node.js applications.

Truffle Framework: To work with ethereum smart contracts, truffle is a strong tool.It provides a platform for testing automated contracts, manages networks and packages, and is used to compile, install, and link smart contracts. [12].

Ganache: Earlier known as Testrpc Ava Gananche is available as both a command-line and a graphical user interface. Ten typical Ethereum addresses are created on a virtual blockchain, and each is preloaded with 100 simulated ether using the private key. Ganache instead automatically confirms each transaction rather than relying on mining. It is practical for OSs including Windows, Linux, and Mac. [13].

Metamask: Metamask is user friendly tool,it is also open source tool having a graphical user interface for doing transactions in ethereum.Without a fully functional Ethereum node running your system browser, Ethereum Decentralized-apps can function. In essence, Metamask serves as a link between browsers and the Ethereum network [12].

Solidity: Solidity is a high-level language with JavaScript style syntax for contracts. This produces machine-level EVM code and transforms it into straightforward instructions.. It has four value types namely: Boolean, Integer, Address and String but has same operators as that of JavaScript [14].

1) working: The voter can access the voting website and log in using the Chrome Extension of Metamask to connect to the local blockchain. After connecting, the page will refresh, revealing the list of candidates and their current vote count after the admin has initiated the election. The voter can has to register with a cryptographic hash from ganache, if they have imported a wallet in metamask. Select a candidate and click the ”vote” button. A Metamask pop-up will appear displaying the Ethereum transaction that needs to be confirmed. If the voter has not voted before, their vote will be counted for the selected candidate once the transaction is confirmed. If the voter has already voted, attempting to vote again will result in a failed transaction, and the vote will not be counted. Ganache is used to deploy a local blockchain, and metamask is configured to communicate with it. The Truffle framework enables the migration of solidity-based smart contracts to a local blockchain. When a user clicks to vote, Metamask enables them to transfer Ether across accounts. Each user has a distinct identifier known as an Ethereum Address, a private key, and a certain amount of Ether is distributed to each voter’s account in specific amounts.. When we launch the project, all the transactions will be accessible to everyone once the voting is completed by the user, the Ether or amount is transferred from the voter’s account to the candidate’s account, and all transactions go through the blocks.. This will give voters complete transparency and they can cross-check their votes. Once the voting is done by the user, the amount of Ether is changed in the address,as there is record of this transaction if the user try to vote one more time, the transaction is not considered and the vote will not be counted

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023
ISSN: 2583-6129
DOI: 10.55041/ISJEM00423
www.isjem.com
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

2 *User Interface:* User interface is through which users can interact with the e-voting system. The picture bellow is how user will see the interface. The loading screen will continue to display loading until the electorate login through metamask.

When voters log in using Metamask, the screen below will be shown.

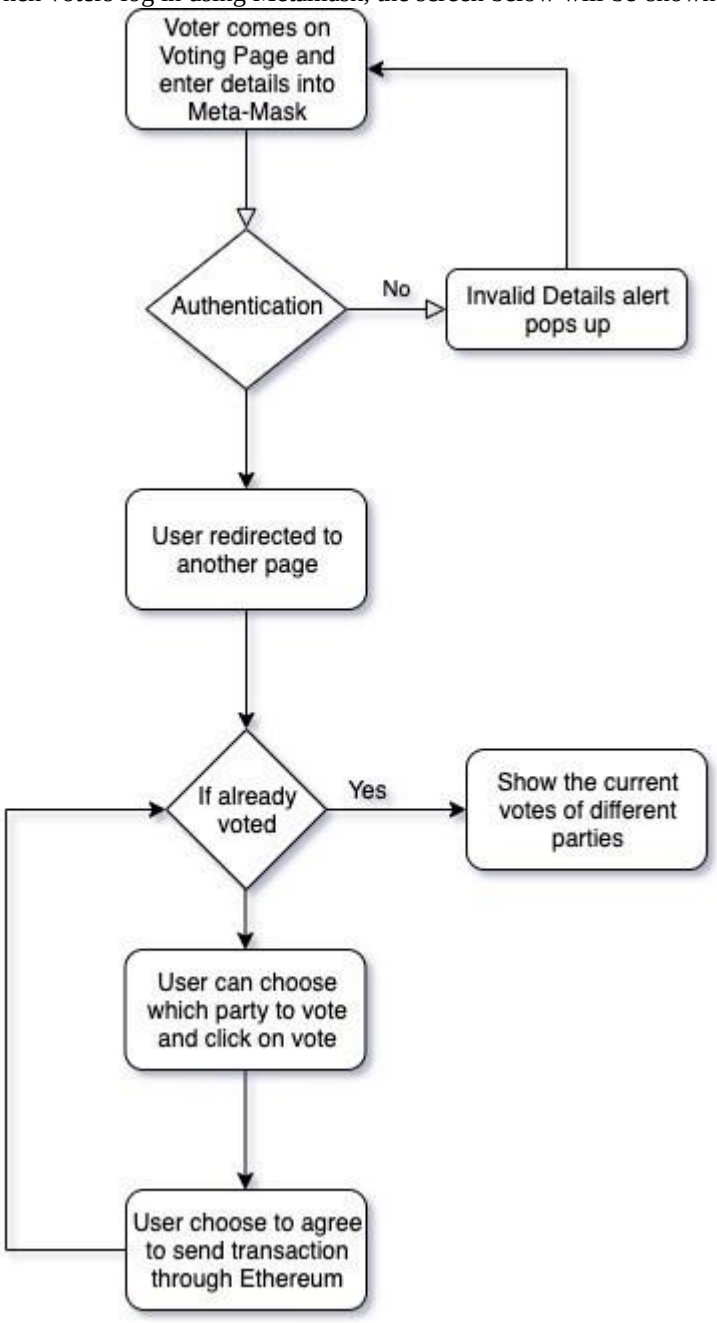

Fig. 4. Flow model of the E-voting system based on blockchain

Now, we utilise the truffle framework and a command line to upload the smart contract to the blockchain. NPM directory has also been utilised by command. For this, the commands listed below are utilised:

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

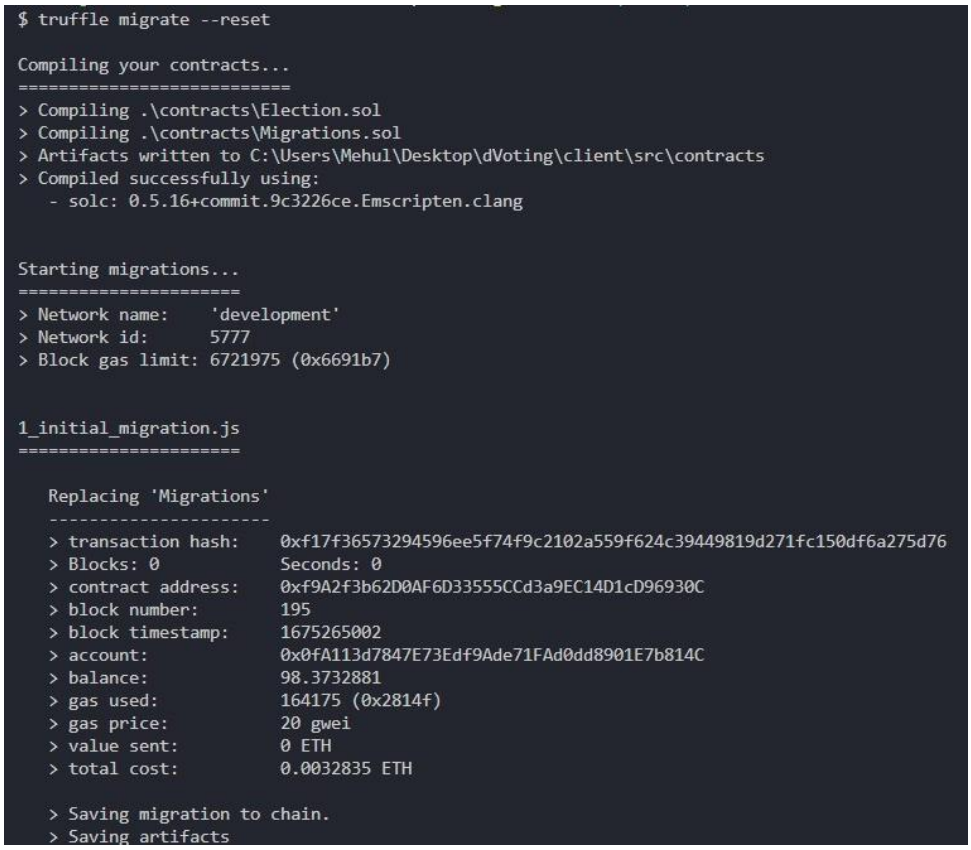

Fig. 5. Snapshot of Command Line for Truffle Framework

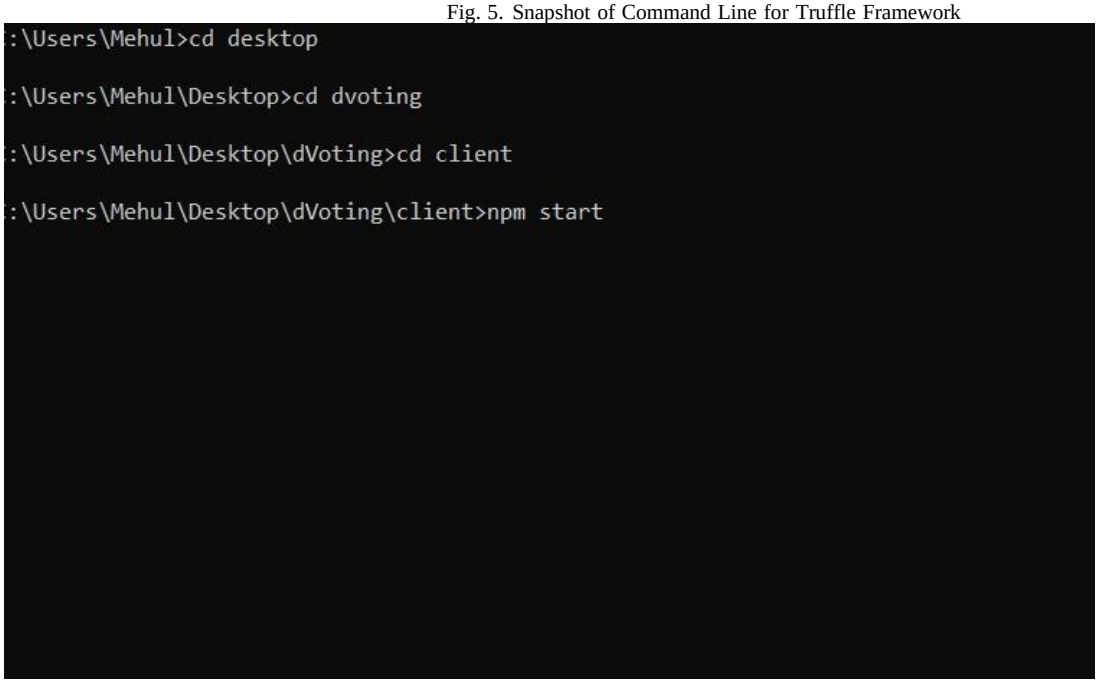

Fig. 6. Command Line of NPM Directory

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

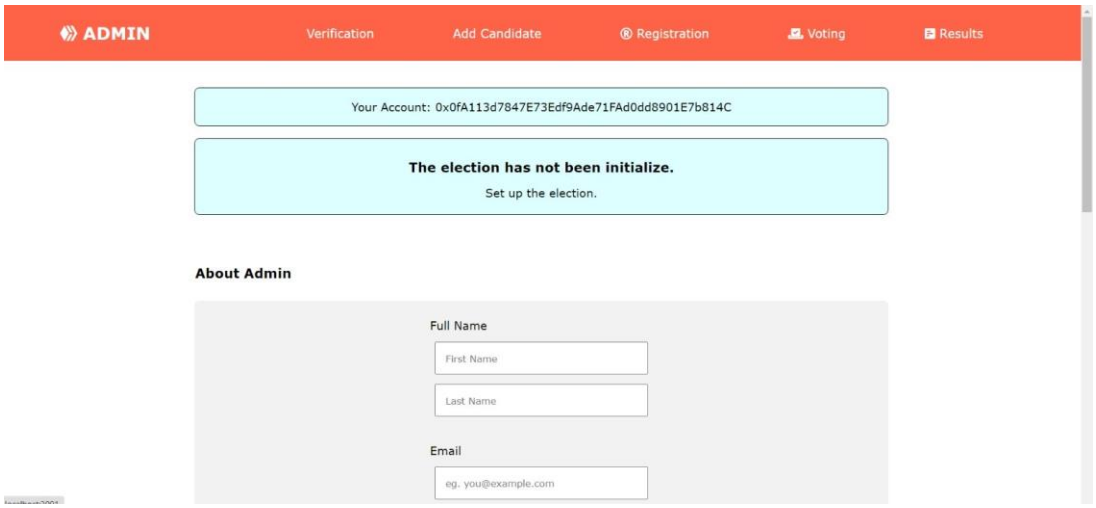

Fig. 7. Working of frontend module

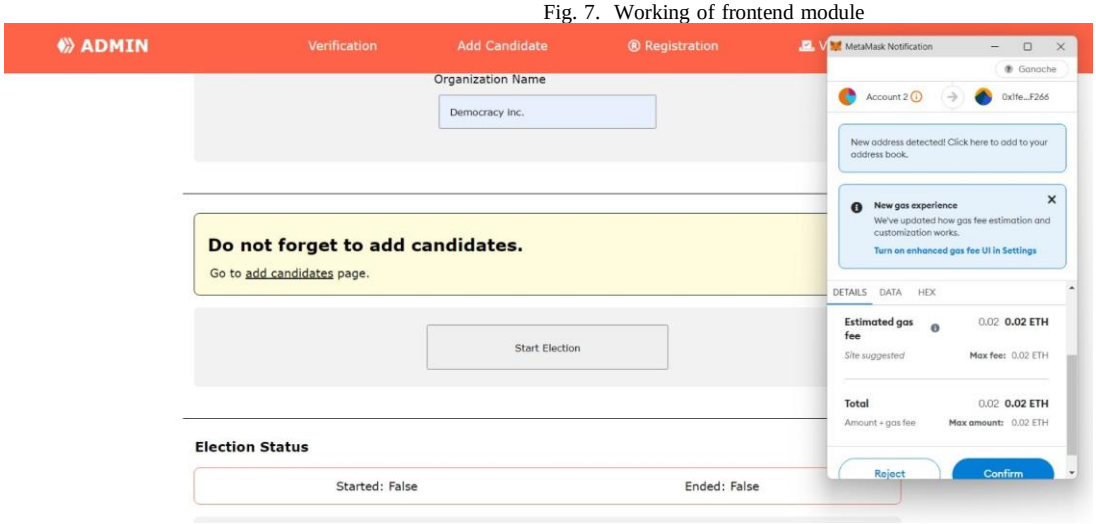

Fig. 8. Working of frontend module

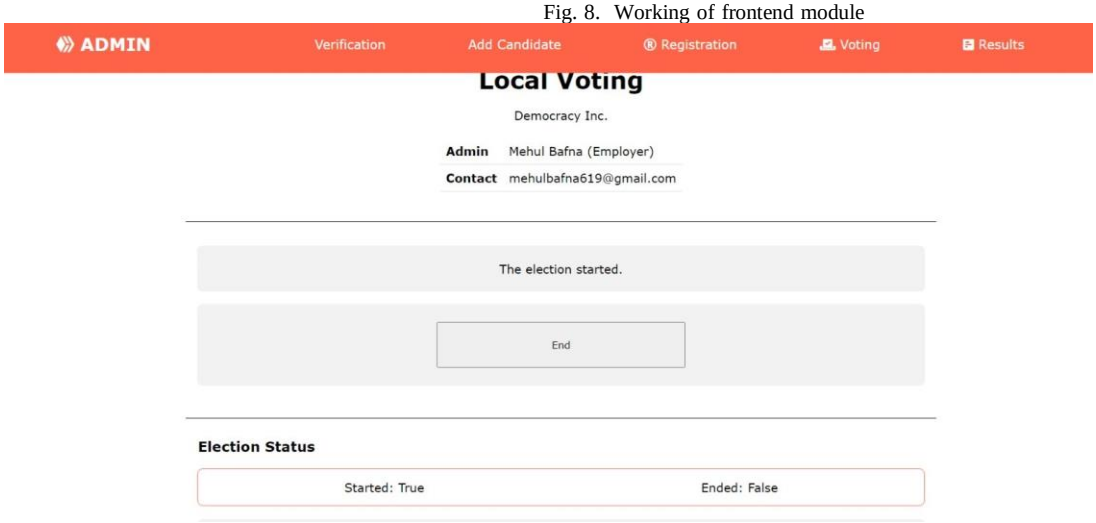

Fig. 9. Working of frontend module

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

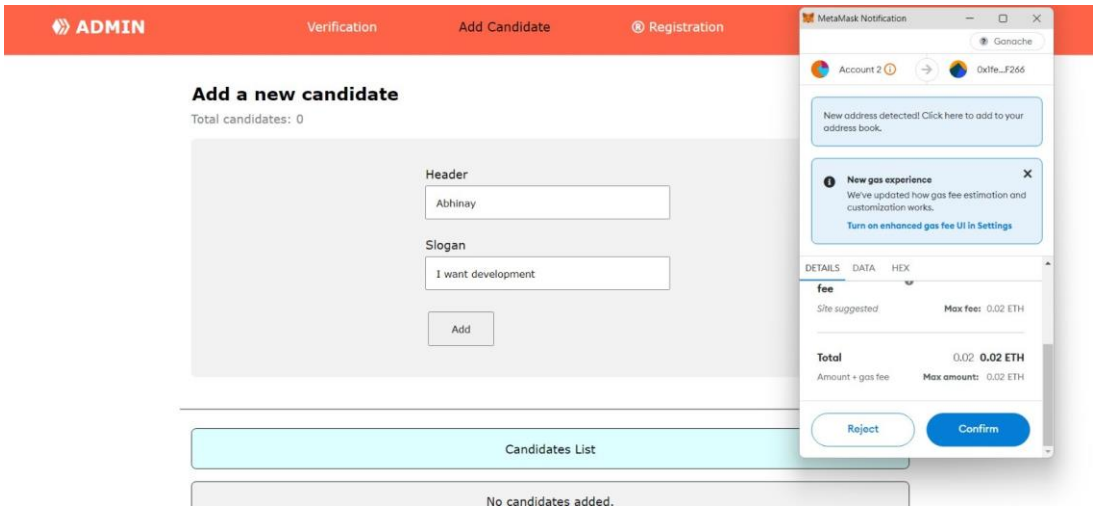

Fig. 10. working of frontend module-adding canditate

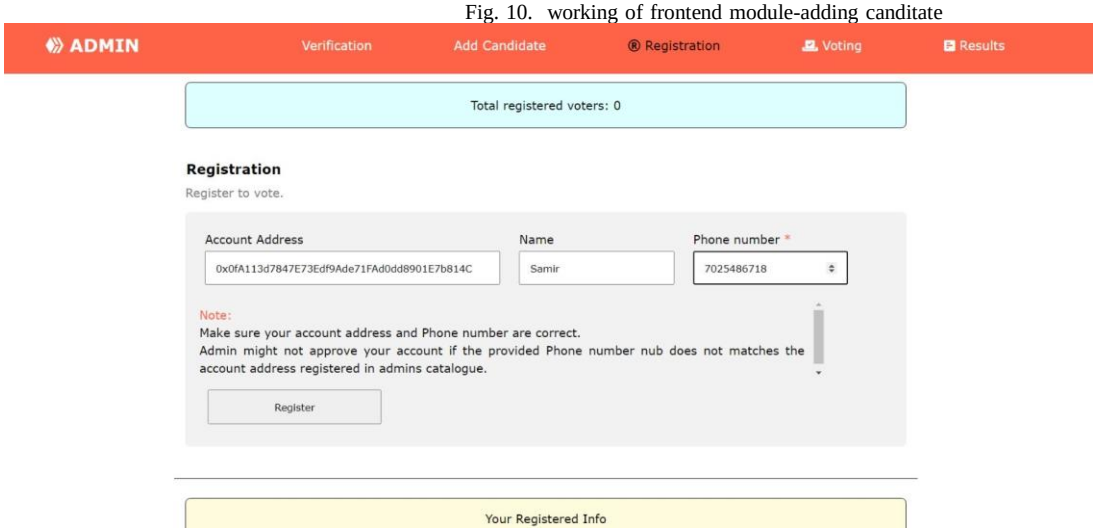

Fig. 11. Working of frontend module-voter registration

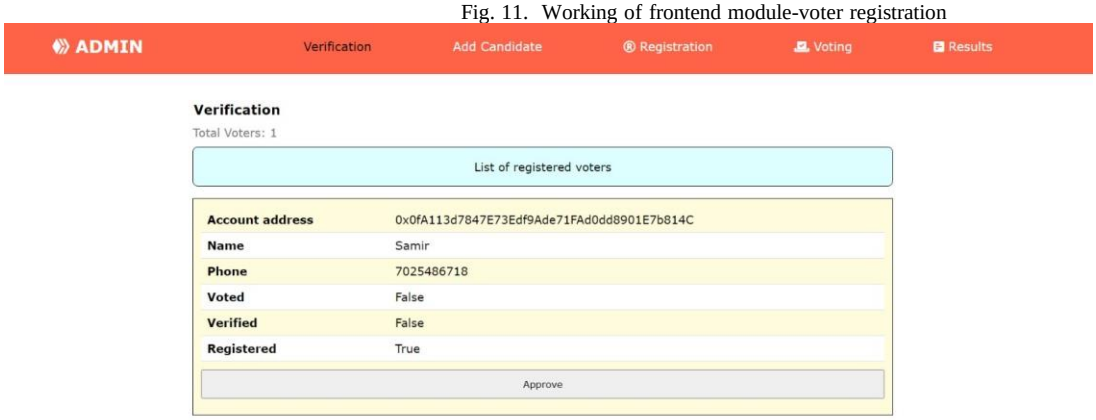

Fig. 12. Working of frontend module-voter registration

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

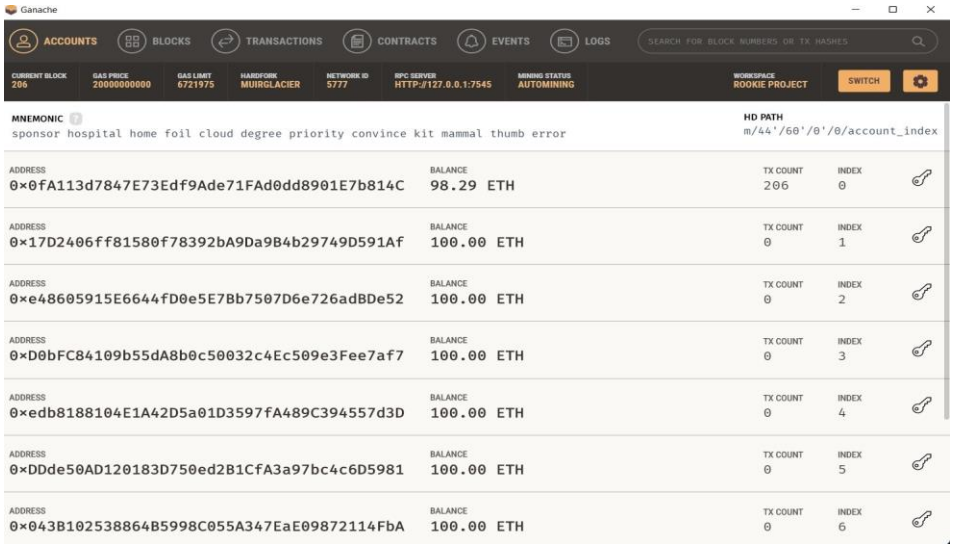

Fig. 13. Ganache Interface

Fig. 14. Ethereum development account address

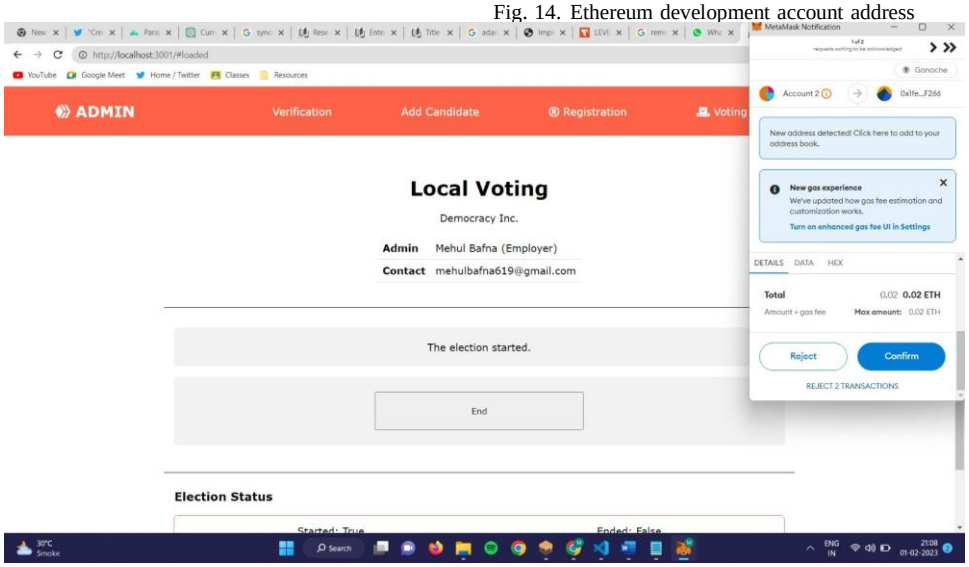

Fig. 15. Working of frontend module-admin interface

International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI: 10.55041/ISJEM00423
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

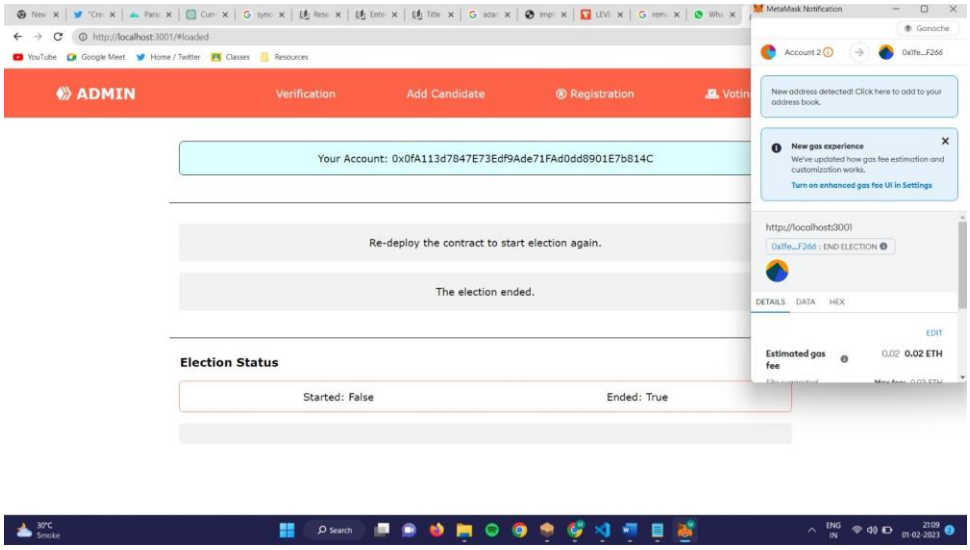

Fig. 16. Working of frontend module-admin interface

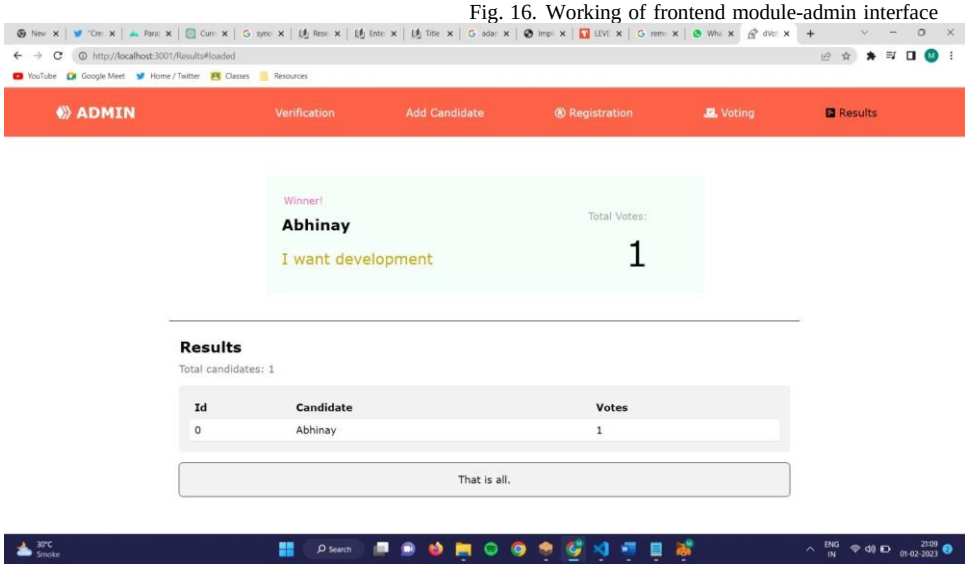

Fig. 17. Working of frontend module-election result

IV. Conclusion

Blockchain technology is a new innovation in voting systems that has shown to be more trustworthy and accurate than previous methods since it is safe, secure, and time and cost effective. In this study, we employed blockchain-based electronic voting with smart contracts, which provide a set of guidelines for how parties should communicate and decide on contracts. For implementation, a variety of technologies like Ganache, the Truffle framework, NPM, and metamask were utilised. Blockchain technology is decentralized, making it possible to moderate and change such systems. By enabling users to connect to a system with an intuitive user interface so they may cast their vote, our suggested method offers convenience to voters.

References

[1] https://shermin.net/token-economy-book/
[2] JZhang, S.Wang, L. Xiong, H. Int. J. Inf. Secure(2019) Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. International Journal of Information Security. https://doi.org/10.1007/s10207-019-00465-8
[3] E. Elewa, A. AlSammak, A. AbdElRahman, T. ElShishtawy, ”Challenges of Electronic Voting-A Survey”, Advances in Computer Science: an International Journal, vol. 4, no. 6, pp. 98-108, 2015.
[4] Aranha DF, Ribeiro H, Paraense ALO (2016) Crowdsourced integrity verification of election results. Annals of Telecommunications:1–11. doi:10.1007/s12243-016-0511-1
[5] Gjøsteen K, Lund AS (2016) An experiment on the security of the norwegian electronic voting protocol. Annals of Telecommunications:1–9. doi:10.1007/s12243-016-0509-8
[6] Budurushi J, Renaud K, Volkamer M, Woide M (2016) An investigation into the usability of electronic voting systems for complex elections. Annals of Telecommunications pp 1–14. doi:10.1007/s12243-016-0510-2
[7] Neumann S, Volkamer M, Jurlind B, Prandrini M (2016) Secivo: a

ISSN: 2583-6129
DOI: 10.55041/ISJEM00423
www.isjem.com

quantitative security assessment model for internet voting schemes.
Annals Telecommunication pp 1–14

[8] Ayed, A.B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. International Journal of Network Security Its Applica- tions (IJNSA) Vol.9, No.3, May 2017

[9] Hsiao JH, Tso R., Chen CM., Wu ME. (2018) Decentralized E- Voting Systems Based on the Blockchain Technology. Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore. Alexander, Steven Lander and Ben Howerton (2018). Netvote:rsA Decentralized on Smart Cities 02 2020 - 06 2020 — Volume 4 — Issue 10 — e4 Voting Network Available at: https://netvote. io/wp- content/uploads/2018/02/Netvote-White-Paper-v7.pdf

[10] https://www.tutorialsteacher.com/nodejs/what-is-node-package-manager

[11] https://www.edureka.co/blog/developing-ethereum-dapps-with-truffle

[12] https://www.codementor.io/@swader/developi ng-for-ethereum-getting-started-with-ganache-l6abwh62j

[13] https://www.edureka.co/blog/solidity-tutorial/