Grenze International Journal of Engineering and Technology, June Issue

Voting System using Blockchain

Anil V Turukmane[1], Jetty Sai Ganesh[2] and Keerthi Sunkara[3]
[1]Professor, School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India
Email: anil.turukmane@vitap.ac.in
[2-3]School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India
Email: saiganesh.20bcr7065@vitap.ac.in, keerthi.20bci7176@vitap.ac.in

***Abstract*—Even though electronic voting significantly decreased election costs and offered some convenience, it has been criticized for being unreliable when compared to the traditional pen and paper method because it is physically possible for someone with physical access to the system to change the results. A central system is also necessary to oversee the entire process, including electronic voting. Election results and tracking of those results. Given how easy it is to target votes, voters are not entirely safe. It also poses a severe danger to voting rights and transparency. This article offers a solution to the problems associated with traditional elections by utilizing blockchain technology, which has become a fascinating technology for various applications due to its distinct qualities that set it apart from other technologies. The aim of this project is to develop a decentralized electronic voting system that verifies voter identity through an honest and transparent voting process and protects voter privacy during data transfer using blockchain technology.**

***Index Terms*— Ethereum cryptocurrency, blockchain, decentralized, and e-voting.**

I. INTRODUCTION

A. E-Voting

Casting a ballot and utilizing a computerized mechanism to count the results is known as electronic voting. Smart cards, diskettes, and tape cartridges are used to hold votes before they are sent to a central site for compilation. Among the voting techniques are touch screens, optical scanners, and direct electronic recording, or DER.

B. There are two main ways to vote electronically:

Voters must queue up to cast their ballots at polling places when electronic voting is conducted on-site. Government officials keep an eye on these equipment. Voters do not need to be present in person to use remote electronic voting, which can be done via polling locations, computers, cell phones, tablets, the internet, text messaging, or polling stations. The security community came to this conclusion based on security concerns. Thought that the computerized voting machines were unreliable and inaccurate. The application is undermined and votes on the system may be impacted by physical access to the device. Elections should be secure and impervious to hacking, regardless of the organization. While voter privacy and confidentiality must be respected, a quick vote count is necessary to prevent suspicions from being raised.

C. Blockchain

Since blockchain creates an immutable and transparent system, it has shown to be a great alternative to the

Grenze ID: 01.GIJET.10.2.576

traditional method. A blockchain is a collection of ordered data that consists of blocks that are linked to each other via a chain. The "genesis block" is the name given to the first block. Every time a new block is added to a blockchain, a stack is produced. Each block consists of data, a hash, and the hash of the block that came before it. A block's hash changes when its contents do, but the hash of the subsequent block is not affected by the hashes of the blocks that came before it, rendering the current block and any subsequent blocks invalid.
This will help you prevent tempering because modifying one block will need you to get the hash for every block that comes after it. On the other hand, hundreds of thousands of hashes may now be computed rapidly by hackers. It avoids this problem by slowing down the creation of new blocks through the use of the proof-of-work concept. A distributed, decentralized peer-to-peer network is also used. Every node in the network receives a newly created block. Each node's blockchain receives the new block after it has been confirmed that no manipulation has occurred. The consensus that is formed when all nodes in the network concur on whether or not a block is real is what gives blockchain technology its reputation for being so reliable, safe, and secure.

D. Smart Contract

A smart contract is a self-imposed agreement in blockchain-controlled computer code. The contract will immediately take effect upon the fulfilment of the previously established guidelines. A set of guidelines that govern the parties' communication and decision-making about the contract are contained in this code. Because of the architecture that smart contracts offer, tokenized assets and access rights can be successfully governed by two or more parties [1]. A smart contract's operation is illustrated in Fig. 1 [1]. Smart contracts allow blockchain technology to be expanded and used similarly to an immutable database.

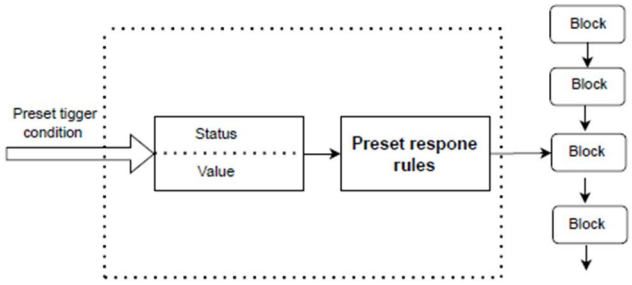

Figure 1. Smart Contract Working Principle

A smart contract has several facets, such as technological, legal, and economic ones, which can be understood as:
Smart Contract Features:

Technical Aspects:

- Self-executing (enforcement on the go) and Self-verifying (auditing on the fly)
- Unchangeable (no lying or deception)

Legal Aspects:

- Smart contracts allow automated procedures to be connected to legal obligations.
- When implemented correctly, they can result in increased contractual security.

Financial Considerations

- Reduced transaction costs; • Greater openness; • Fewer intermediaries

By examining the data, a smart contract's terms can be independently verified. The contract developers won't have to worry about overseeing contract execution since each node in the network will ensure that a single contract is executed correctly. Written into code, smart contracts are self-executing contracts between many parties. This implies that using smart contracts, legal responsibilities could be transformed into automatic processes. It is possible for the contract to begin automatically due to an expiration date or another trigger. This article outlines the implementation of a blockchain technolog based electronic voting system that addresses e-voting's issues and builds voter confidence in order to enable valid voting. It will be a positive step for the growth of intelligent government. Section 2 provides an brief view of recent research on blockchain technology and voting systems; Section 3 suggests an electronic voting system based on blockchain technology; and Section 4 provides the operational details and findings. There are four components to this study.Our work is ultimately concluded in Section 5.

II. Related Work

The widespread adoption of the electronic voting system marked a significant improvement over the traditional pen and paper method. Election procedures in many nations now feature electronic voting. The system offered a number of advantages, including as increased voter turnout, accountability, cost-effectiveness, and flexible election scheduling, but there were also a variety of serious issues. A variety of issues pertaining to electronic voting systems were covered by Abdelwehab et al. [3] in their study, including assaults, technological difficulties, social and cultural barriers, and legal considerations.

In an attempt to boost transparency and voter turnout in computerized elections, Diego F. Aranha et al. [4] discovered an experiment to validate the correctness of election results. The two primary elements of this idea were the electoral authorities using crowdsourcing to validate election results and voters using mobile devices to collect pole tape at different locations. Election results cannot be hacked provided voters follow the voting processes correctly, according to Kristian Gjosteen and Anders Smedstuen [5], who provide a statistical method to improve voting security.

Budurudhi et al. [6] look at the proper architecture of voting machine interfaces and the use of such interfaces for complex elections in an effort to promote voter and electoral administrator involvement. Since voting verification is a critical concern, it is argued that the interface offered by remote voting technology presents significant issues. These issues have an effect on votes. To protect desirable property during remote electronic voting, a great deal of work goes into developing and validating voting protocols with encryption.

A model for comparing voting schemes in any electoral environment was developed by Neumann et al. [7]. They then applied this model to the specific context of online voting in Estonia and provided recommendations for the optimum kind of voting system for that particular scenario. People began searching for answers because of several problems with electronic voting, especially those related to physical security. This is how blockchain, which was first used with bitcoin, made its way into the electronic voting area. Ahmed Ben Ayed [8] describes in his work how to make electronic voting anonymous, secure, and safe using blockchain technology. The work of Jen-Ho Hsiao et al. [9] employs smart contracts for electronic voting driven by decentralized blockchain technology, allowing every voter to be involved in the tallying and assessment of votes. Both voter confidence and election financing misuse are decreased by it.

NetVote is a decentralized program that was utilized by Jonathan Alexander et al. [10] as the software's user interface in this experiment. With the help of the dApp admin, election administrators may establish voting procedures, register rules, decide on electoral policy, and open and shut polls. Biometric readers and other methods are used for voter identification. TallydApp is utilized for testing and verifying election results. This NetVote enhances the three categories of elections: token-holder, open, and private.

The present electronic voting method has a number of issues that make it difficult to get reliable results, including:

- Hacker-prone.
- Ineffective auditing
- Misreading the intentions of voters.
- Political prejudice on the manufacturer's part.
- Software program tempering.
- Ineffectiveness in getting the votes cast.
- Issues with the hardware, etc.

The primary goal of this project is to create a blockchain-based electronic voting system that fixes the long-standing issue with the legislation. This idea can be applied in a variety of contexts, such as national voting, including offices, colleges, and schools. because fraudulent acts such as running information campaigns, tampering with votes, hacking voting machines, and more frequently endanger elections. Our model will tackle each of these issues.

III. Proposed System

Among other things, the proposed method takes use of ganache, the truffle framework, npm, and metamask. Truffle imports the smart contracts onto the blockchain, whereas Ganache manages the internal blockchain that Metamask may access. To create an account and wallet address, users need Ether, the cryptocurrency used by Ethereum. The user must pay "gas," a predetermined transaction cost, in order to publish the transaction to the blockchain. Votes are cast, and then a number of nodes on the network called miners complete the process.

These miners are competing with each other to complete the transaction. The miners that successfully finish this transaction will receive the ether that users bought to submit their votes.

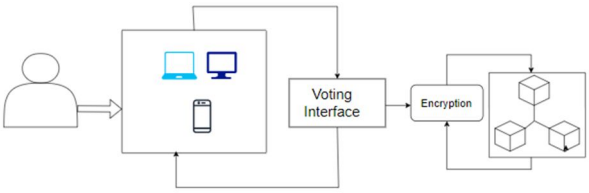

Figure 3: Initial Design of a Blockchain-Based Electronic Voting System

Using 64-bit hardware or a Windows 7 computer or later, NMP dependencies, the Truffle framework, Metamask, Solidity Toolkit, and Ganache, our suggested methodology may be put into practice.

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

NPM (Node Package Manager)

The node.js packages inside of an application are managed, installed, updated, and deleted using the package manager NPM. The tool needs a command line in order to function. The local mode and the global mode are the two unique modes of operation. In local mode, an application's single directory is affected; in global mode, all node.js programs are affected [11].

Truffle

The Truffle framework is a useful instrument for facilitating communication between Ethereum smart contracts. It is used to manage networks and packages in addition to connecting, creating, and deploying smart contracts. Additionally, a framework for automated contract testing is included. [12].

Ganache

You may access both the graphical user interface and the command-line versions. It was once called Testrpc. Ten legitimate Ethereum addresses are created using a fictitious blockchain; a private key preloads 100 ether into each address.

Because Ganache verifies every transaction automatically, mining is not necessary. Linux, Mac, and Windows operating systems all function well with it [13].

Metamask

With a graphical user interface, Metamask is an easy-to-use, open-source program that makes Ethereum transactions easier. You do not need to have your system browser operating on an Ethereum node in order to launch Ethereal Dapps. In essence,

A web browser and an Ethereum blockchain are connected using Metamask [12].

Firmness

Solidity

High-level contract language Solidity has a syntax akin to JavaScript. This technique generates machine-level EVM code and translates it into short instructions. Although its operators are the same as those in JavaScript, its four types of values are Boolean, Integer, Address, and String [14].

Working

The voter can access the voting website, but before he can connect to the local blockchain, he must log in via the Metamask Chrome Extension. When page refreshes, the user-selected candidates and most recent votes are shown. The candidate's voting option is below that. Following selection of a candidate and "Vote," the user is notified of the Ethereum transaction that has to be finished via a metamask pop-up. If a person has never voted before, they cast their vote for the chosen candidate. Once a user has cast a ballot, they cannot do so again, and their vote will not be recorded. Meta mask is set up to link to a local blockchain that Ganache installs. Using the Truffle framework, it is possible to migrate Solidity smart contracts to the local blockchain. Meta mask enables cross-account Ether transfers when a user clicks to vote. Each voter's account receives a unique Ethereum

address, or ID, for them, together with the exact quantity of Ether. After a vote, ether is moved from the voter's account to the candidate's account. Once the project is up, all of the transactions are accessible to everyone and are routed through blocks. Voters will be able to verify their ballots twice thanks to complete transparency.
When a user tries to vote again, the transaction will fail and the vote will not be recorded since the address will not have the same amount of Ether as before. While every other node mines, we have allowed Ganache to mine automatically on other nodes' behalf in this particular case. The voting part of the procedure is explained in the flowchart below.

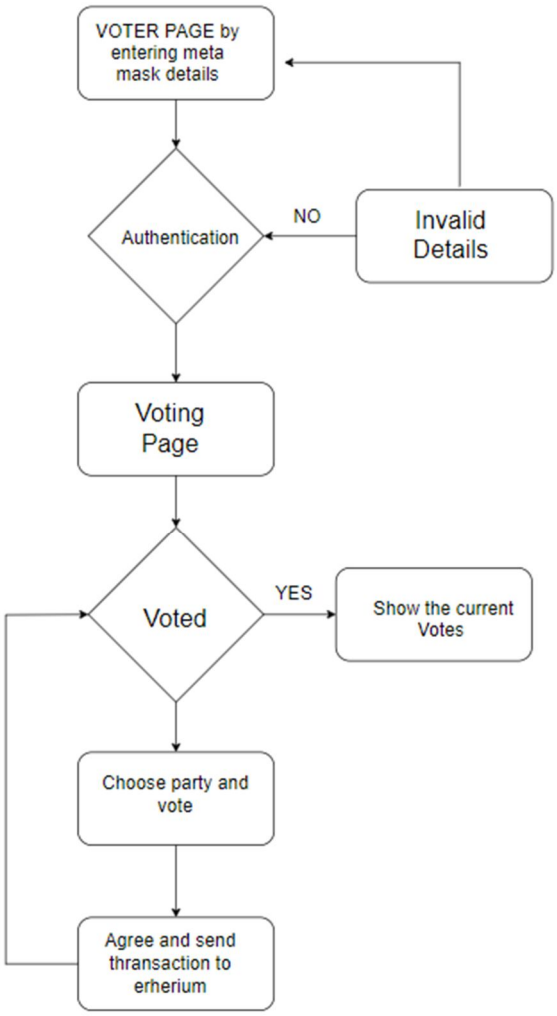

Figure 4: Blockchain-based electronic voting system flow model

IV. RESULTS

Compared to traditional electronic voting techniques, the blockchain-based electronic voting system that is being suggested offers several advantages. Voter security and integrity are enhanced by blockchain's decentralized design. Because distributed ledger technology creates an unchangeable record of transactions, it lessens the possibility of manipulation or tampering by a single party. Consequently, the electorate gains credibility, which is crucial for maintaining the legitimacy of election outcomes.
Furthermore, by automating the application of voting criteria, the use of smart contracts lowers the requirement for manual processes and the risk of bias or human error. By employing transparent, immutable protocols, smart contracts increase the accountability and fairness of the voting process.

In addition, the technique preserves voter confidentiality while enabling voters to verify that their votes were accurately recorded. Finding this delicate balance between openness and privacy is essential to preserving voter confidence and engagement.
It is simpler to construct the proposed system across several election levels, from local to federal, by utilizing generally accessible technologies such as Ganache, Metamask, and the Truffle framework.

V. Conclusion

In conclusion, the challenges raised by conventional electronic voting methods can be addressed by the suggested blockchain-based electronic voting system. The technology promotes confidence among interested parties and enhances the legitimacy of electoral proceedings by leveraging the distinctive features of blockchain, including decentralization, immutability, and transparency.
Further research and development are required to address any potential problems and enhance the system in order to get it ready for broader usage. To properly implement and scale up the suggested approach, key stakeholders including governmental bodies, election authority, and technical specialists must work together. Ultimately, blockchain-enabled electronic voting has the power to totally alter democratic procedures and ensure future election outcomes that are safer, more transparent, and more transparent.

References

[1] https://shermin.net/token-economy-book/
[2] Zhang, S., Wang, L. & Xiong, H. Int. J. Inf. Secur. (2019) Chaintegrity: blockchainenabled large-scal 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 VotingA 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 [1] Ramkumar Devendiran, Anil V Turukmane, Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy, Expert Systems with Aplications, Volume 245, 2024, 123027, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2023.123027. (https://www.sciencedirect.com/science/article/pii/S0957417423035297)
[8] Anil V Turukmane, Ramkumar Devendiran, M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning,Computers & Security, Volume 137,2024, 103587,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2023.103587.
[9] G. Khekare, C. Masudi, Y. K. Chukka and D. P. Koyyada, "Text Normalization and Summarization Using Advanced Natural Language Processing," 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2024, pp. 1-6, doi: 10.1109/ICICACS60521.2024.10498983.
[10] G. Khekare, S. Ghugare, R. Khatri, G. Majumder and U. Khekare, "Blockchain Powered Integrated Health Profile and Record Management System for Seamless Consultation Leveraging Unique Identifiers," 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 2024, pp. 1-9, doi: 10.1109/ic-ETITE58242.2024.10493266.
[11] Ganesh Khekare, K. Pavan Kumar, Kundeti Naga Prasanthi, Sanjiv Rao Godla, Venubabu Rachapudi, Mohammed Saleh Al Ansari and Yousef A. Baker El-Ebiary, “Optimizing Network Security and Performance Through the Integration of Hybrid GAN-RNN Models in SDN-based Access Control and Traffic Engineering” International Journal of Advanced Computer Science and Applications(IJACSA), 14(12), 2023. http://dx.doi.org/10.14569/IJACSA.2023.0141262.