2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) | 979-8-3503-2579-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAISS58487.2023.10250609

Blockchain-based Voting System in a DemocraticEnvironment

Nitin Sai Varma Indukuri
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana
indukurinithin5@gmail.com

Sridhar Reddy Eguram
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana
sridhar.eguram@gmail.com

Anil Nichena
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana
mudirajanil96@gmail.com

Suhas Ulvalapudi
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana
renny.suhas@gmail.com

Dr. Ramesh Gajula
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telangana
ramesh680@gmail.com

Abstract--**Voting is one of the fundamental concepts that help the people of a democratic country exercise their right to choose their leader. One way to securely conduct voting is through electronic voting systems. It acts as a digital platform that eliminates not only the need of using paper for casting votes as well as the need to gather in person. By providing each voter with a unique ID, the platform helps maintain the integrity of a vote by preventing multiple votes by the same person. An electronic voting system also comes with some obvious advantages over a paper-based approach, them being increased efficiency and reduced errors. The electronic voting system not only improves accuracy but also provides enough flexibility for the voters by facilitating the process of voting. It does so by allowing the voters of a country to vote from anywhere at any time if they have an internet-connected device. Blockchain allows for a distributed and decentralized technology with very powerful cryptographic functionalities that provide promising methodology for our Voting System. Utilizing Blockchain technology can help us relieve some concerns with the present voting systems such as fraud, multiple votes, etc.**

Keywords – Ganache, MetaMask Wallet, Ether, Truffle IDE, Smart Contracts, Ethereum Blockchain Network, Cryptocurrency, Democracy, Election

I. INTRODUCTION

India is a democratic, sovereign nation. As the trend of digitalization doesn't seem to be slowing down, every Indian citizen has become a part of a growing digital India with a unique digital ID called Aadhar Card [5]. Voting procedures have changed from early systems that relied only on human counting to ones that now use paper ballots, punch cards, and electronic voting machines.

Blockchain is a cutting-edge technology that utilizes robust cryptographic principles to facilitate secure solutions for various applications. It operates as a data structure that securely records and shares all transactions from its inception. Essentially, it serves as a decentralized database, ensuring the integrity of continuously evolving data records by safeguarding them against unauthorized manipulation, tampering, and revision [6]. Through blockchain, users can connect to the network, initiate transactions, validate them, and generate new blocks. Every block in the chain is allocated a hash value, which gives the block a unique identity [7]. The value of the hash doesn't change as long as the data in the block is unchanged. However, any modifications made to the block will result in an immediate change to the hash, indicating potential malicious activity or unauthorized changes to the data. Consequently, the robust cryptographic principles employed in blockchain technology have made it a popular choice for combating unauthorized transactions in diverse fields.

This study explores the potential of utilizing blockchain in electronic voting to ensure anonymous voting, vote integrity, and verifiability. It is known that e-voting systems can benefit from essential features provided by the blockchain. Some of these include using cryptographic hashes for the validation of transactions by itself and the use of a distributed ledger for records. The inherent characteristics of blockchain, including preserving anonymity, decentralized maintenance, and public distribution of transaction ledgers among all nodes, make it a valuable tool in the field of electronic voting. This technology proves highly effective in addressing threats such as double spending of voting tokens and attempts to manipulate result transparency.

II. LITERATURE SURVEY

There are several articles and research works which explains about the security issues of e-voting system in the blockchain domain:

According to “Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L.” [7], the author elaborates on decentralized anonymous voting system i.e.: It only requires a minimal level of confidence between participants, making it suitable for large-scale elections. The lack of a legitimate third-party authority for defense raises several issues about the system's ability to survive Denial-of-Service (DoS) attacks, which are highlighted in the article.

From “Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System” [8], the author focuses on how blockchain technology offers a workable way to get around these issues. It demonstrates how conventional voting systems rely on a central figure who, in the absence of adequate verification, is readily controlled or modified. Contrarily, systems based on blockchain store data across numerous nodes, making it nearly hard to hack or modify every node at once. Votes cannot be revoked thanks to their decentralized character, and their efficient verification may be carried out by contrasting them with those of other nodes. However, there are certain limitations that the privacy where user can only obtain information about voter’s choice.

A blind signature is used in the voting system suggested by Fujioka, Okamoto [9]: A voter renders his vote sightless before forwarding it to the validator [10]. The ballot is returned to the voter when the validator signs it and confirms that the user is authorized to cast a ballot. The tallier then verifies the validator's signature before approving the ballot when the voter creates a signature for the transparent vote and transmits it to him or her.

According to “Ayed and Ahmed Ben” [11], authors believe that voters will cast their ballots via a secure device. However, there’s a limitation that even though their system is secure, hackers have the capacity to use malicious software that has been pre-installed on the device that the voter is going to use to cast or alter a vote [12]. The author system's inability to reverse a vote in the event of a user error is one of its drawbacks.

III. EXISTING SYSTEM

At present, the electoral system relies on manual operations. This leads to inefficiencies as voters are required to visit multiple polling locations to cast their ballots, resulting in wasted time. This prevents many individuals from voting, which is one of the most significant and worrying factors. Every vote matter in a democracy. There is a need for an up-to-date electronic voting system that can be used to increase efficiency and transparency while simultaneously limiting vote frauds.

Limitations of Existing Systems:

- The present voting system has a single controller that monitors the entire voting process in a particular area. In the case of the controller’s dishonesty, this can lead to erroneous elections.
- There is a lot of waste of time and resources on behalf of the voters for this present election process which makes it an obstacle for many voters to exercise their right to cast a vote.
- This present election system might also be subject to ethical concerns such as use of muscle to influence, multiple votes, etc.

IV. PROPOSED SYSTEM

The proposed system has been specifically developed to cater to the needs of a practical voting system, considering crucial factors such as confidentiality, eligibility, ease of use, vote secrecy, and trustworthiness. The primary objective of the proposed system is to ensure secure digital voting while maintaining user-friendly functionality. To achieve this, the system incorporates a web interface that promotes user commitment. Additionally, measures like fingerprinting are implemented to prevent instances of double voting. Recognizing the importance of managing voters, constituencies, and candidates, an administrator interface is incorporated to ensure easy access and a seamless user experience.

The requirements upon which we based the proposed system are:

- Preserving Confidentiality - Safeguarding the secrecy of an individual's vote
- Eligibility - Enabling exclusive participation from registered voters, ensuring that each eligible voter can cast a single vote.
- Preserving vote secrecy - Voters should lack the ability to provide evidence to any external party regarding their chosen voting preferences.
- Ease of use - Ensuring that voting is convenient for all eligible individuals, allowing every eligible voter to participate.
- Ensuring trustworthiness - Establishing the capability to have confidence in the process of tallying votes.

V. METHODOLOGY

The proposed system avoids instances of double voting by employing a web interface to encourage user commitment by incorporating procedures like fingerprinting, using a unique id or iris data. A user-friendly interface is implemented for the administrator that can be used to manage voters and candidates effectively while ensuring convenience. Additionally, the proposed system promotes equal participation rights for all voters, fostering an unbiased and legit environment for competition among candidates while preserving voter identity. As proof of casting the vote, the hash of the transaction is emailed to the voter, allowing tracking of the vote outside the constituency premises if necessary.

A. User Interaction:

The Front-End plays a crucial role in facilitating interactions with both voters and administrators. It encompasses two essential roles: user authentication and authorization. These rules ensure that only authorized users, according to the arranged guidelines, are granted access to the electronic voting system. A multitude of techniques can be employed to achieve this, ranging from uniquid/password authentication to more advanced techniques such as thumbprinting or iris scanner. While the specific implementation depends on isolated architecture, we are utilizing a Unique ID for this study. Ultimately, this layer serves as the initial point of contact for users and verifies their credentials based on system-specific policies. The voting process from the perspective of the user is shown in Fig 1.

B. Synchonizing Ledger:

We synchronize the ledger with the specific database application used, i.e MySQL inorder to export data from the blockchain onto the local system. The results are stored on the applciation in order to allow voters to track their vte wth they Unique ID number.

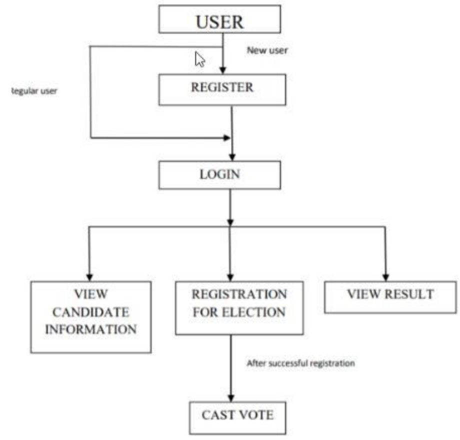

USER
New user
Regular user
REGISTER
LOGIN
VIEW CANDIDATE INFORMATION
REGISTRATION FOR ELECTION
VIEW RESULT
After successful registration
CAST VOTE

Fig 1: User Interaction Flow

C. Voting System:

Usually, a voter accesses the system by providing their Unique ID for authentication. If the Unique ID entered by the user matches another in the database, a list of candidates is shown to the voter so that he can cast a vote to their desired candidate. However, if no match is found for the Unique ID presented by the candidate, then further access is refused.

The votes cast by the users undergo confirmation by various miners. By employing blockchain and hashes, verified votes are added to the ledger while maintaining end-to-end verification. Consequently, blockchain conders a cast vote as a transaction within the system. The transaction is appended to the existing blocks as a new block while consequently being records in the back-end database. The system ensures the vote integrity principle of democratic voting systems by utilizing the unique ID of each voter, which is checked at the inception of every attempt at voting to prevent multiple voting.

Following the validation process, the voter promptly receives a notification via message or email containing the transaction ID defined earlier. This allows the user to track their vote within the ledger. The hash assigned to each voter serves as their unique identifier within the blockchain, facilitating the overall verifiability of the voting process. Importantly, this hash remains hidden and inaccessible to anyone, including system operators, ensuring the privacy of individual voters.

VI. IMPLEMENTATION

The proposed system has been implemented in an isolated environment, utilizing a web-app as the user interface to facilitate user interactions in an appropriate manner. The application is developed using JavaScript and hosted on the Truffle IDE, which serves as the data source for the application. The backend database employed is MySQL, where the admin manually inputs various data such as voter details, constituency information, and details of political parties participating in the election. In order to document votes that are in the form of transactions, we have integrated Ganache as a platform which creates a private blockchain network specifically for this system. The choice of Ganache was influenced by its user-friendly features, allowing for seamless integration into our proposed architecture.

VII. DEPENDENCIES

A. Ganache:

Ethereum, despite its very wide functionality, can be very expensive to use in the primitive stages of development. The primary functionality of Ganache is to emulate a private Blockchain network to interact with our smart contracts to develop and test decentralized applications using blockchain. Some of the features provided by Ganache are:

- Displays blockchain log output.
- Comes with advanced mining control.
- Has a built-in block explorer.
- Provides an Ethereum blockchain environment.
- It not only includes a Desktop application but also a command-line tool.

B. MetaMask Wallet:

MetaMask is a free web and mobile crypto wallet that helps users store and exchange cryptocurrency, interact not only with the Ethereum Blockchain network but also with the local Ganache network for deployment of our Decentralized Voting System. It is said that some of the functions provided by MetaMask are:

- Crypto Storage: Tokens created using Ethereum's ERC-20 and ERC-721 token standards may be kept in MetaMask's built-in crypto wallet, and users can quickly create and switch between different wallet addresses inside the app.
- Token Swaps: Peer-to-peer (P2P) token swaps may be carried out using MetaMask's trade feature right from your wallet.

- Access to decentralized Applications: Users of MetaMask may employ the wallet to instantly access a range of Ethereum-based dApps, cryptocurrency lending operations, games, NFTs, and more.

C. Truffle IDE:

With the purpose of reducing the work of programmers, Truffle is the best programming IDE as it provides an environment for testing, and consequently acts as an asset pipeline for blockchain running on the Ethereum Virtual Machine [13].

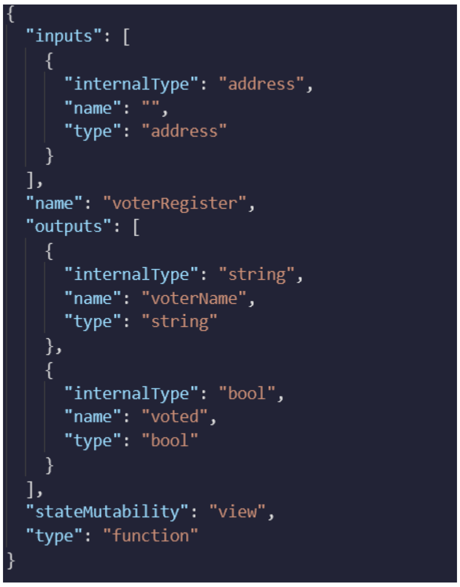
- Integrated compilation, linking, and deployment of smart contracts.
- Automated contract testing for rapid development.
- Scriptable, extensible deployment & migrations framework.
- Deployment of multiple public and private networks using the built-in Network Management tool.

- Interactive console for direct contract communication.
- Configurable build pipeline with support for tight integration.
- An External Script runner is used to run static scripts on truffle.

VIII. RESULT WITH ANALYSIS

The evaluation aimed to assess the system's performance based on e-voting system requirements and identify considerations for its real-world application. The experimentation involved multiple steps, including conducting transactions, verifying them, mining them into the blockchain, propagating ledger changes to all network nodes, and assessing system usability. A test run was performed directly on Ganache, starting with the casting of a vote.

In the duration of a vote being transferred, a hash is generated to record the event. The vote is seen on the receiving node as the balance increases by a value of one. We can notice a transaction being recorded in a JSON file in Fig 2. The transaction can now be seen on the ledger, which indicates that the attempt to mine has been successful. Our system is designed to allow each address to have a maximum of one vote, ensuring that voters cannot double vote unless the node receives them from a separate address.



```
{
  "inputs": [
    {
      "internalType": "address",
      "name": "",
      "type": "address"
    }
  ],
  "name": "voterRegister",
  "outputs": [
    {
      "internalType": "string",
      "name": "voterName",
      "type": "string"
    },
    {
      "internalType": "bool",
      "name": "voted",
      "type": "bool"
    }
  ],
  "stateMutability": "view",
  "type": "function"
}
```

Fig 2: Transaction

IX. CONCLUSION

Ever since the dawn of technology in the 1970s, e- voting has been employed in many ways, offering significant advantages over paper-based systems by improving efficiency and reducing the frequency of errors. The rise of blockchain [15] has prompted an upper hand in investigating the viability of blockchain as a solution for effective electronic voting. This research study focuses on one such endeavour that capitalizes on the advantages of blockchain, including cryptographic principles and transparency, to establish an efficient e-voting solution. The approach that has been put forward can be used successfully using Ganache, and a comprehensive assessment of the methodology underscores its potency in meeting the essential requirements of a blockchain-based e-voting system.

X. FUTURE WORK

Future endeavors, persists in implementing and refining the proposed system, while also conducting further research to enhance its performance. Nevertheless, there are additional features that can be integrated into the proposed system. Some of the changes that can be possibly to the system includes:

- Add features where system administrator can start and stop voting through a front-end application built using React.
- Make a dedicated database where the details of the users such as Name, Address, Aadhar Card and Voter ID can further be linked to the Ethereum address.
- Try to find a blockchain network other than Ganache that is cost-efficient to deploy the app on a wider scale.
- Enhance the resilience of blockchain against the "double spending" issue [14].

Primary objective revolves around creating a more efficient and advanced system for E-voting by harnessing the potential of blockchain technology and its associated tools.

. REFERENCES

[1] Taylor C. Boas; Voting for Democracy: Campaign Effects in Chile's Democratic Transition; Latin American Politics and Society (2018)

[2] Emad Abu-Shanab, Michael Knight and Heba Refai; **E-voting systems: a tool for e-democracy;** Management Research and Practice (Vol. 2, Issue 3)

[3] N Kersting, H Baldersheim; Electronic Voting and Democracy: a comparative analysis (2004)

[4] A. Khandelwal, "Blockchain implementation on E-voting System," *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, India, 2019, pp. 385-388, doi: 10.1109/ISS1.2019.8907951.

[5] Roopak T M, Dr. R Sumatthi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology". Department of Computer Science and Engineering, Siddaganga Institute of Technology 2019.

[6] David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb,2018 "Decentralized Voting Platform Based on Ethereum Blockchain", Department of Computer Science American University of Science and Technology

[7] Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L. Date: A decentralized, anonymous, and transparent e-voting system. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018.

[8] Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*. 2021; 21(17):5874. https://doi.org/10.3390/s21175874

[9] Fujioka, A.; Okamoto, T.; Ohta, K. A practical secret voting scheme for large scale elections. In Proceedings of the International Workshop on the Theory and Application of Cryptographic Techniques, Queensland, Australia, 13–16 December 1992. [Google Scholar]

[10] Mohammadpourfard, M., Doostari, M. A., Ghaznavi Ghoushchi, M. B., and Shakiba, N. (2015) A new secure Internet voting protocol using Java Card 3 technology and Java information flow concept, *Security Comm. Networks*, 8, 261– 283, doi: 10.1002/sec.978.

[11] Ayed and Ahmed Ben, "A conceptual secure blockchain-based electronic voting system", International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01-09, 2017\

[12] Ben Ayed, Ahmed. (2017). A CONCEPTUAL SECURE BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM. 10.5121/ijnsa.2017.9301.

[13] Farnaghi, M., & Mansourian, A. (2020). Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS. *Cities*, *105*, 102850. https://doi.org/10.1016/j.cities.2020.102850

[14] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 52, 3, Article 51 (May 2020), 34 pages. <https://doi.org/10.1145/3316481>

[15] G. Ramesh, Avinash Sharma, D. V. Lalitha Parameswari, Ch. Mallikarjuna Rao & J. Somasekar (2022) Blockchain in healthcare : Moving towards a methodological framework for protecting Biomedical Databases, Journal of Discrete Mathematical Sciences and Cryptography, 25:4, 891-901, DOI: 10.1080/0972052