Securing Democracy: Blockchain-based E-Voting Systems for Enhanced Security

Krishna Varma, Mayur Mahajan, Prateek Meshram, Tejas Purohit, Rishabh Waghmare

Student, Student, Assistant Professor, Student, Student
Computer Engineering,
Dr. D. Y Patil Institute of Engineering, Management, and Research, Akurdi, Pune, India

Abstract *Election could be an important event during a trendy republic still massive sections of society around the world don't trust their election system that's a major concern for the republic. Indeed, the world's largest republics like the Republic of India, The US, and Japan still suffer from a blemished legal system. Vote apparel, hacking of the EVM (Electronic vote machine), election manipulation, and cell landing square measure the crucial problems within the current electoral system. during this system, we tend to square measure work the problems within the election vote systems and try to propose the E-voting model which might resolve these issues. Blockchain in the distribution of the database voting systems can reduce one of the infidelity sources of database manipulation and increase the voting security among the voters. The physical voting systems have multitudinous excrescencies in it as well as the digital voting systems are not perfect enough to be executed on a large scale. Blockchain could be an unquiet technology of the current period and guarantees to enhance the adaptability of e-voting systems. this fashion presents a shot to influence edges of blockchain like cryptological foundations and translucency to attain an effective theme fore-voting. The projected theme conforms to the essential musts fore-voting schemes and achieves end-to-end verifiability. The system presents an in-depth analysis of the theme that with success demonstrates its effectiveness to attain an Associate in Nursing end-to end empirical e-voting theme.*

Keywords: Blockchain, Smart Contract, Cryptological, EVM, Voting System

1. INTRODUCTION

The security of elections is a matter of utmost importance for every democracy. Over the past decade, the field of computer security has extensively explored electronic voting systems to reduce the cost of national elections while enhancing their security measures. Since the inception of democratic processes, voting systems have relied on traditional pen and paper methods. However, replacing the conventional approach with a modern election system is crucial to combat fraud and ensure traceability and verifiability in the voting process [7][8]. Voting serves as an abecedarian medium for collaborative decision- timber and expressing opinions within a group or electorate. Traditionally, voting has been intertwined with debates, conversations, and the vehemence of choices. Over time, ultramodern republics have transitioned from traditional ballot-grounded systems to electronic voting(e-voting), with some difficulties girding the trust ability of Electronic Voting Machines (EVMs) and their reported irregularities in election issues.[7] securing the integrity of choices is a matter of public security for every republic. In the realm of computer security, experts have considerably explored electronic voting systems, aiming to reduce the cost of public choices while upholding and enhancing security measures. Historically, the legal frame for choices has reckoned on pen and paper, but the need for a new voting system arises to combat fraud, ensure traceability, and corroborate the voting process. still, electronic voting machines have faced scrutiny from the security community due to enterprises about physical security, as unauthorized access could manipulate the machine and alter the vote count.[19] This is where blockchain technology comes into play. A blockchain, with its distributed, inflexible, and transparent nature, provides an implicit result to address these challenges in the realm of choices. In this paper, we discuss DApp of Voting system using blockchain technology, a secure and user-friendly system that ensures transparency of the voter while voting and robust functioning.[1][2]

2.RELATED WORK

Shahzad et al. (2019) proposed a new framework to improve e-voting with blockchain. It introduced a proof of completeness algorithm, addressing block development, locking, and information management. The presiding officer would verify voter ID and biometrics, and the voter would cast their vote. A hash using SHA-256 would be generated and sent to the officer to create a block. However, additional measures are required to ensure security, privacy, and transparency, establishing it as a reliable voting method **(Toapanta et al., 2019).**

Dagher et al. (2018) introduced Bronco Vote, a blockchain-based voting technology for universities. It enhances transparency, protects voter anonymity, and reduces costs. The system utilizes Ethereum's smart contracts and three contracts—Registrar, Creator, and Voting Contract—to manage elections. However, registration security is a concern, potentially allowing unauthorized access.

In **Nir Kshetri's** research, each voter is treated as a wallet, and transactions between wallets are limited. Candidates are receiver wallets, making voting a transaction between them. Blockchain-enabled e-voting with encrypted keys and tamper-proof IDs ensures secure and transparent voting, reducing violence and improving accuracy. However, it lacks a decentralized system and consensus mechanism. The wallet-coin model could be enhanced by using a single wallet instead.

In **Jorge Lopes' (2019)** research, Jorge Lopes proposed a blockchain-based e-voting system utilizing smart contracts. The system involves three entities: director, developer, and voter. It consists of three contracts: Record, Creator, and Election. The Record contract stores voter registration securely. Funds are transferred to the Creator Contract for initiating an Election Contract. The ballot is encrypted using homomorphic encryption before being added to the blockchain for confidentiality and security.

4. LITERATURE REVIEW

Adida, B., Helios (2008). "Web-based open-audit voting.", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008. This paper proposes associated justify an adequate security model and criteria to judge comprehensibility. It additionally describes a web ballot theme, pretty graspable Democracy, show that it satisfies the adequate security model which it's a lot of graspable than Pretty smart Democracy, presently the sole theme that additionally satisfies the planned security model.

Dalia, K., Ben, R., Peter Y. A, and Feng, H. (2012). "A fair and robust voting system by broadcast.", 5th International Conference on E-voting, 2012. This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot secrecy.

The authors in [24] proposed a methodology of combining the secret sharing scheme and homomorphic encryption with the blockchain to build up a decentralized e-voting framework without a trusted third party. Moreover, the framework provides a transparent voting manner while preserving the anonymity of the voter's identity. The author during the billing phase preserves the data transmission privacy and verifies the ballots.

2. PROBLEM STATEMENT

The problem addressed in this project is the need for a secure and transparent e-voting system using blockchain technology. Existing e-voting mechanisms lack efficient identity verification and suffer from multiple registrations. This project aims to develop a system where administrators can initiate elections, add candidates, and verify registered voters. Through the use of smart contracts and decentralized applications, voters can securely cast their votes, ensuring transparency and preventing multiple voting instances. The goal is to create an accessible and tamper-resistant platform that guarantees fair and credible election results.[2][17]

3. PROPOSED SYSTEM

The proposed system for the e-voting project incorporates smart contracts on the blockchain to facilitate the voting process. Administrators have the authority to initiate and manage elections, add candidates, verify registered participants, and conclude the voting process. The system enables administrators to create voting ballots through decentralized applications, define candidates and constituencies, and deploy them onto the blockchain. Voters can register using a generated private key, which allows them to perform gas transactions via the MetaMask platform for registration.[9] Verification of voters requires gas expenditure by the administrator, confirming the provided voter ID and name. Once an individual casts their vote, it interacts with the secret ballot and is added to the blockchain if the code matches. Each voter can only vote once due to the one-time usability of the generated private key.[21] When the election concludes, the administrator announces the winner, and voters can view the results on the website. The actual architecture involves the admin creating a voting instance on a blockchain network, allowing users to register and receive approval to participate in the election. Voters cast their votes, and the admin ends the election, displaying the results. The paper also includes screenshots of the website for clarity.

4. METHODOLOGY

While carrying out a blockchain empowered electronic democratic framework we consider existing and past e casting a ballot framework. Different cycles of characterizing jobs assessing structures, security and lawful issues ought to be considered. We have called the system designed as EVOTE and it will always be so mentioned throughout the paper. It aims to provide a real time online application that can be used to vote on selection of any size. It will aim to work not only voting processes that take place in organizations but also in them villages, suburbs and elections at the national level. Also, we have tried to keep the application as simple as possible in order can work on older systems like the ones on its villages. In our electoral system we have defined the election as a smart contract. So, in our network the choice is agreement between participating nodes. And the wise a defined contract includes defining each role participant, election process and terms and conditions during the election process [10][2]. Every participant must be defined for a specific role. Most people can be given the same role either a different role.

a) **Administrators**

Administrators will oversee all operations of election. They can be given creative tasks the election is valid, see the votes that determine the time period close selection and calculation and disclosure of results.

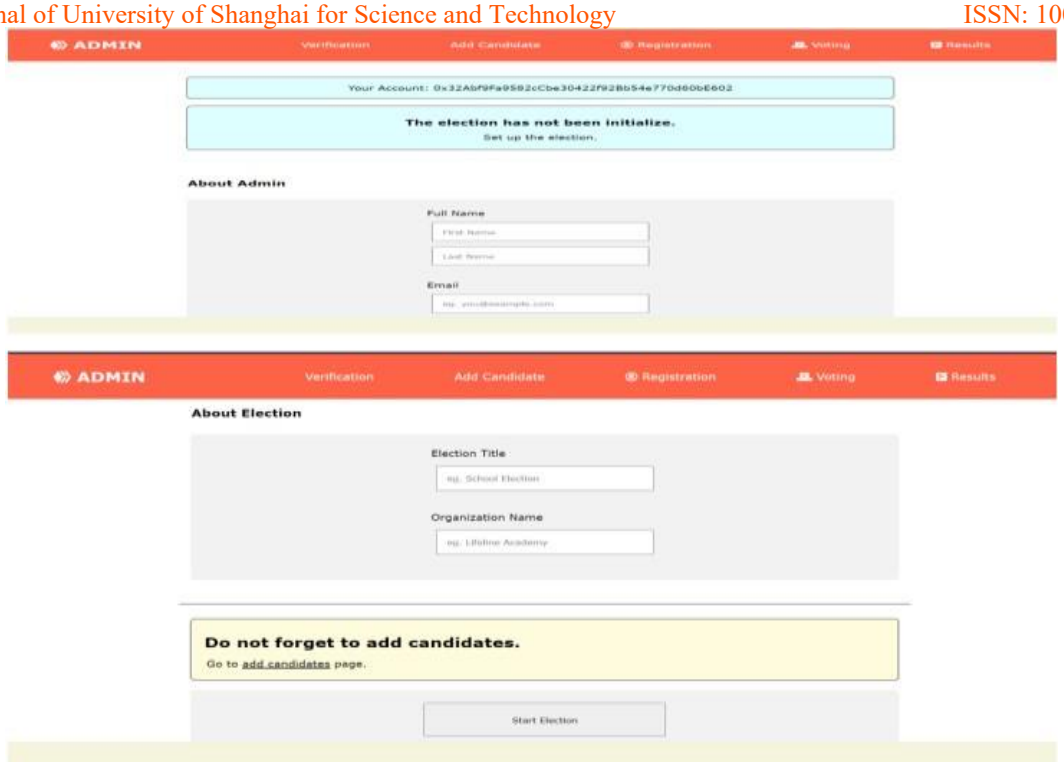

Figure 1. Admin Page

b) **Add candidate Section by Admin** –

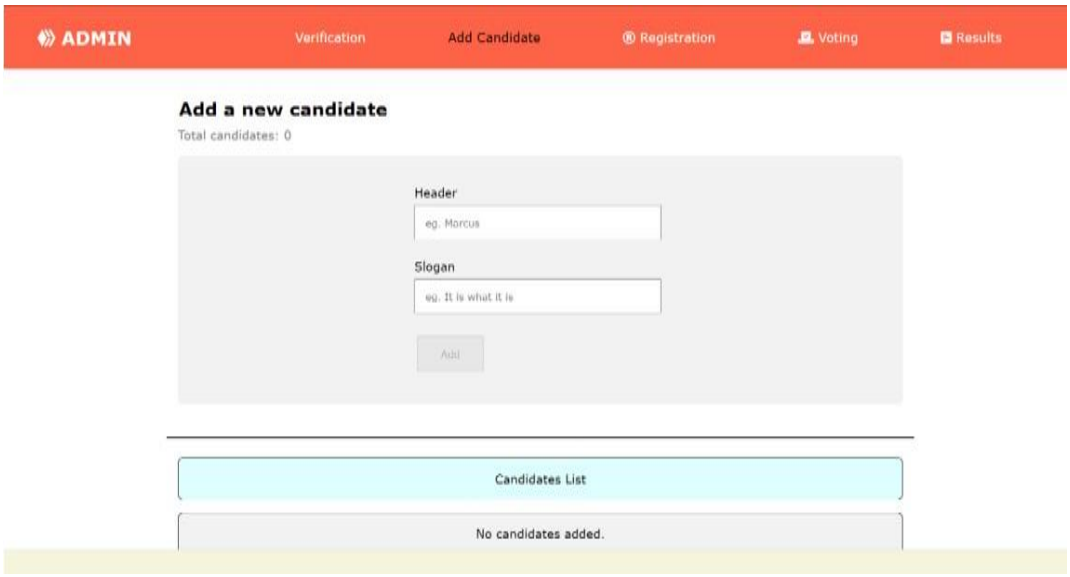

Figure 2. Add Candidate Page

c) **Voters and its registration process for voting -**

A voter is a primary participant who cast a vote in an election. A voter can verify his or her eligibility and self-certification and upload election votes. They can vote and confirm the vote they cast.

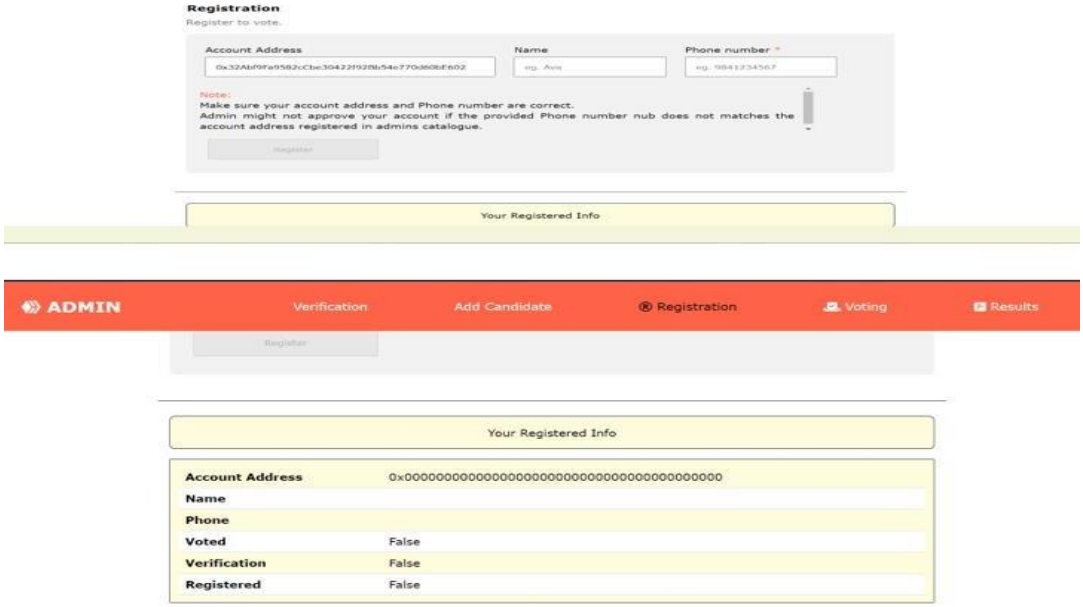

Figure 3. Voter Registration Page

Figure 4. Voting Page

d) **Election Results** –

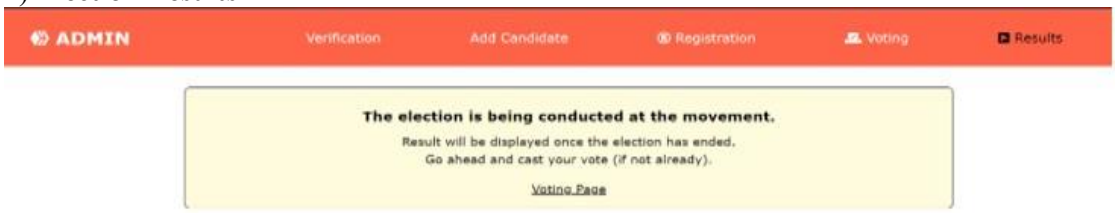

Figure 5. Result Page

e) **Backend data on Sepolia Test Network** –

The e-voting project utilizes a blockchain-based backend infrastructure on the Sepolia test network. The project incorporates a smart contract, which is assigned a unique contract address. The backend system stores essential transaction details, including voter registration, voting results, and election initiation transactions. Additionally, every MetaMask activity associated with the project is recorded and visible on the backend server. This ensures transparency and enables easy tracking of the project's progress, as all transactions can be monitored using Etherscan. By leveraging the power of blockchain technology, the e-voting project aims to enhance the security, integrity, and accountability of the voting process.

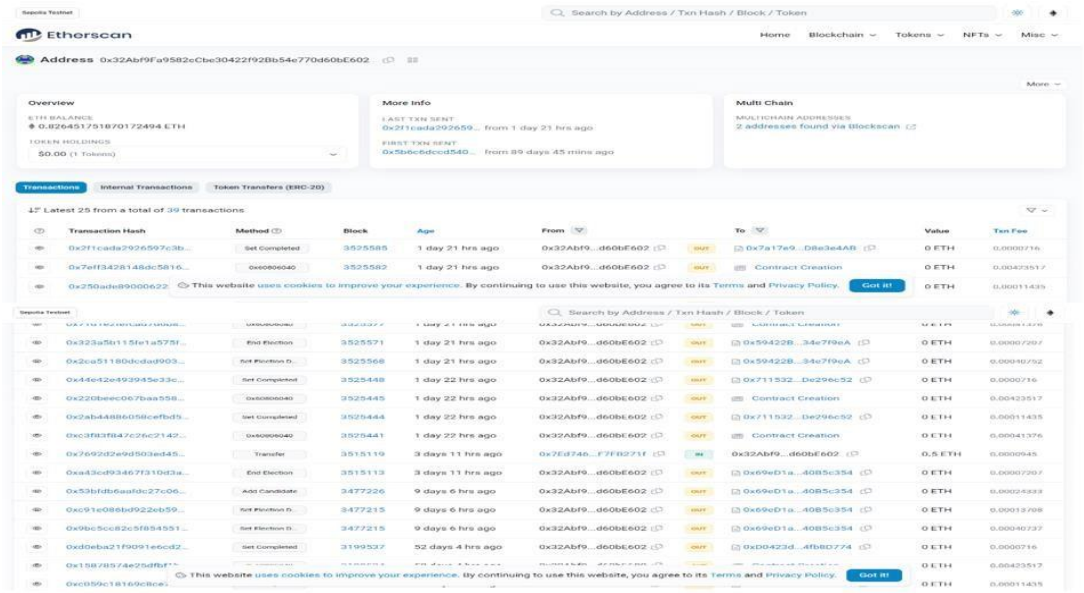

Figure 6. Backend Data on Sepolia Network

f) **Main Coding Zone and Login Details** –

1. **Sepolia Test Network Implementation** – Developer can run project both in localhost and an any private or test network like Sepolia.

2. **Login Details and processor** – The e-voting project incorporates web3 or blockchain technology and utilizes MetaMask as the means of accessing the application. MetaMask acts as a gateway to the decentralized application (DApp) by securely storing and managing the user's private key. In this particular project, the MetaMask private key of an admin has been added to grant the necessary access and authority. This login detail and processor setup ensures a secure and authenticated environment for administering the e-voting system. The private key and mnemonic are stored in “env” and “secrets. json”.

truffle-config.js

```
const path = require("path");
const {mnemonic, projectId } = require('./secrets.json');
const HDWalletProvider = require('@truffle/hdwallet-provider');

module.exports = {
  // See <http://truffleframework.com/docs/advanced/configuration>
  // to customize your Truffle configuration!
  contracts_build_directory: path.join(__dirname, "client/src/contracts"),
  networks: {
    development: {
      network_id: "*",
      host: "127.0.0.1",
      port: 7545, // for ganache gui
      port: 8545, // for ganache-cli
      // gas: 6721975,
      // gasPrice: 20000000000,
    },
    sepolia: {
      provider: () => new HDWalletProvider(mnemonic,
`https://sepolia.infura.io/v3/${projectId}`),
      network_id: 11155111,
      gas: 5500000,
      confirmations: 2,
      timeoutBlocks: 200,
      skipDryRun: true,
    }
  },
};
```

Figure 7. Sepolia Network Implementation

5. IMPORTANT TERMS

Election as a smart contract: In our political decision framework we have characterized a political decision as a shrewd agreement. So, in our organization, the political decision is the arrangement between the participating nodes. When the smart contract is characterized, it incorporates characterizing the jobs of every member, the cycle of political decisions, and terms and conditions inside the election process.

Election Process: The voting process is done by the arrangement of smart contracts gets that are empowered into the blockchain. Smart contracts are characterized appropriately for jobs characterized by the members of the organization. The administrators have the ability to commence the election, add the candidates, verify the registered candidates, and end the elections. Administrators can also create voting ballots by means of decentralized applications. An admin can also define the candidates and voting constituencies. The smart contract makes and develops the election and is published into the blockchain. This voting process consists of multiple procedures in it. The voter can also register through the registration tab with the help of a private key that will be generated at the administrator server.[5] With the help of that private key, the voter enables the gas transaction through the MetaMask platform and registers himself. For verification of every user, the admin has to use the gas in other words, ethers as a transaction cost. Verification is done with respect to the voter id and name that is provided at the time of pre-registration.[13] When an individual voter casts his/her vote, they interact with the secret ballot. The smart contract interacts with the blockchain and if the code is matching, then the vote is added. A voter once cast a vote, has no permission to cast another vote. This is because the private key generated will work only once per individual. Once the election is ended, the announcement of the winner is very crucial. Since the whole process is carried out digitally, the number of votes cast to an individual is counted automatically and the administrator ends the polling. Now each voter can view the result on the website in their systems.

Architecture of project: The admin will produce a voting example by launching the system in a blockchain network (EVM), also produce an election system, and start the election with the details of the election filled in (including campaigners for users to vote). Also, the likely users connect to the same blockchain network register to become a user to vote for the candidate. Once the voters successfully register, their personal details are shown in the admins' panel (i.e., the verification area). The admin also checks if the enrollment

information (blockchain account transaction data, user name, and phone number if available) is valid and matches his record. If yes, then the admin approves the registered voter making them eligible to take part and cast their personal vote in the election. The registered voter following the confirmation from the admin casts their vote for the campaigner (from the voting site). After some time, depending on the scale of the election the admin ends the election from the admin panel by clicking on end election. As that happens the voting is off and the results are displayed on the result page for users. Here is the outline of the working process of our project in the form of architecture. We are also going to attach screenshots of the working website to make it clear for the viewers of this paper and the real project.

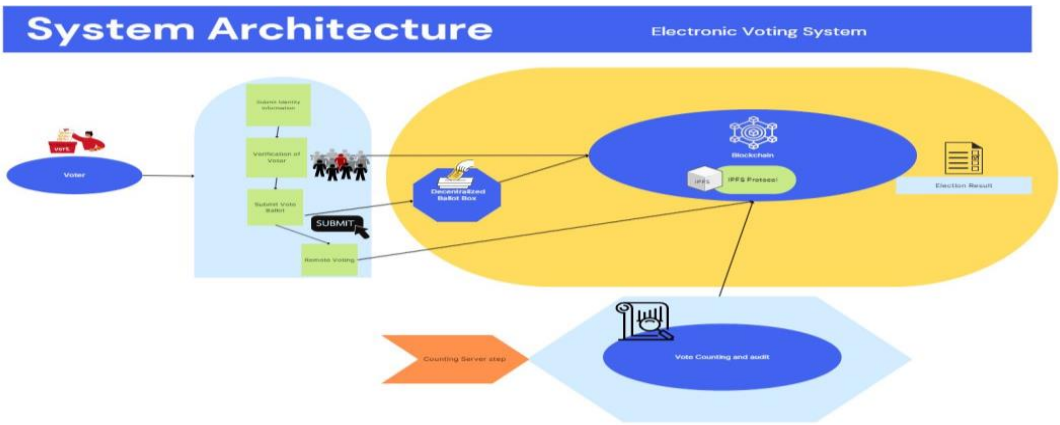

Figure 8. Architecture Diagram

6. UML DIAGRAMS

- **Class Diagram -** The class diagram for the above project represents the relationships and interactions between different classes in the e-voting system. It includes classes such as Voter, Admin, Candidate, Election, Blockchain, Smart Contract, and UI. The diagram illustrates how these classes interact, showcasing the flow of data and functionalities within the system, providing a visual representation of the project's structure and organization.

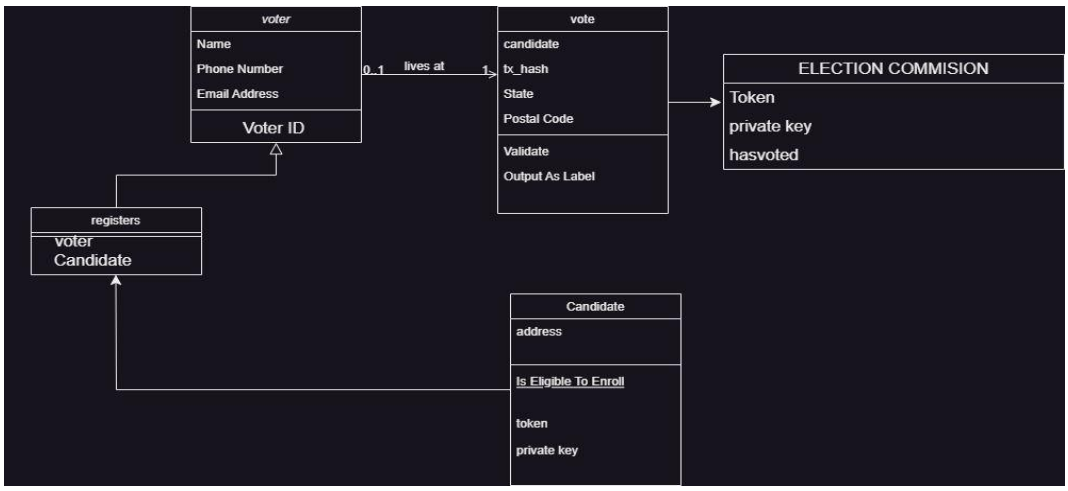

Figure 9. Class Diagram

- **Sequence Diagram** - The sequence diagram for the above project illustrates the flow of interactions between different components and actors. It starts with the administrator initiating the election and creating an instance. Users connect to the system and register as voters. The administrator verifies and approves the registrations. Registered voters cast their votes, which are validated and recorded by the smart contract on the blockchain. Finally, the administrator ends the election, and the results are displayed for viewing by the voters on the website.

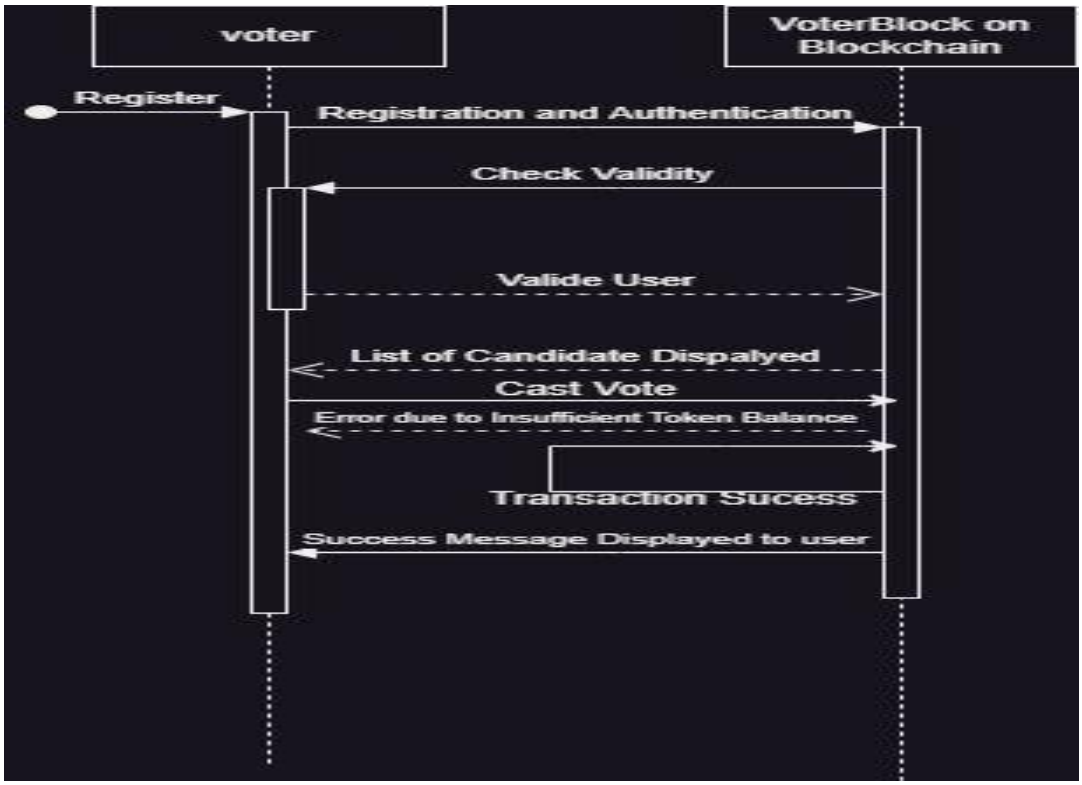

Figure 10. Sequence Diagram

7. FUTURE WORK

A successful e-voting system requires several key features to balance out. Security and privacy issues are undoubtedly one of the most critical factors because we want to avoid being able to manipulate the outcomes of any adversaries or self-interested parties and maintain election integrity. We believed that blockchain had improved some of the security and privacy aspects. However, we can still develop more functionality for this project as we grow in this field.

The future scope of e-voting systems using blockchain technology is promising, especially with the inclusion of Aadhaar card numbers during voter registration. This integration helps prevent multiple registrations, ensuring a fair and transparent voting process. Integrating Aadhaar card numbers adds an extra layer of identity verification and enhances credibility. Aadhaar cards are widely recognized as valid identification documents, making them reliable for voter verification. By linking Aadhaar card numbers to individual voters, the system ensures that only eligible individuals cast their votes, further improving the integrity of the electoral process [2][15]. Blockchain technology also improves efficiency by automating the entire voting process through smart contracts, reducing administrative burdens and costs associated with traditional methods. Overall, this combination holds great potential for secure, transparent, and tamper-resistant elections.

Details of Hardware and Software:

1) Software Requirements

- OS: Windows 7 and above
- Framework: Visual Studio, Remix IDE, Ganache, Truffle
- Server: Sepolia Test Network, Localhost
- Backend: Blockchain and Sepolia Etherscan

2) Hardware Requirements

- Processor: Intel Quad core 1.7 GHZ Processor or above.
- HD: Minimum 10 GB of HD.
- RAM: Minimum 8 GB of RAM

8. CONCLUSION

In conclusion, blockchain technology has gained significant attention in decentralized application systems due to its decentralized nature and robust security features. It offers a unique approach to storing, distributing, and updating data, and is poised to play a crucial role in shaping the future of interactive internet systems [2]. This paper has discussed the development of an e-voting project and presented a final product idea, while also comparing the contributions of recent researchers in addressing security and privacy concerns associated with existing blockchain-based e-voting mechanisms. If we use an Ethereum private blockchain as an alternative for test network, it is possible to send hundreds of transactions or data per second onto the blockchain for the voting system, utilizing every aspect of the smart contract to control the load [14] on the blockchain.

However, it is important to acknowledge that the increasing demand for security and privacy protections may pose challenges to the widespread adoption of real-world blockchain applications [2]. While blockchain offers strong security measures, ensuring adequate safeguards for sensitive voter information and maintaining privacy in e-voting systems remain ongoing areas of research and development.

In order to accommodate larger countries with higher transaction volumes, specific measures need to be implemented to increase the throughput of transactions per second. One approach is the utilization of a parent and child architecture, as suggested in [27]. This architecture allows for a significant reduction in the number of transactions stored directly on the blockchain, maintaining a 1:100 ratio. This optimization enhances scalability while still ensuring the security and integrity of the network.

The website for the e-voting system is already hosted and operational on Google, accessible through the following address: **https://virtualvoter.netlify.app/.** Users can visit the website to access the functionalities provided by the system, including registration, casting votes, and viewing election results. The website is hosted on a reliable platform, ensuring stability and availability for users to engage in the e-voting process. By utilizing this web address, participants can conveniently access the system and participate in secure and transparent online voting.

REFERENCES

[1] Emre Yavuz; Ali Kaan Koç; Umut Can Çabuk ; Gökhan Dalkılıç (2018) Towards secure e-voting using ethereum blockchain.

[2] Krishna Varma, Mayur Mahajan, Prateek Meshram, Tejas Purohit, Rishabh Waghmare, (2023) – IJNRD = "E-Voting DApp using Smart Contract".

[3] KC Tam, (2018), Transactions in Ethereum

[4] S. Shukla, A. N. Thasmiya, D. O. Shashank and H. R. Mamatha, "Online Voting Application Using Ethereum Blockchain," 2018 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Bangalore, 2018, pp.

[5] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050

[6] Blockchain-Enabled E-Voting Nir Kshetri and Jeffrey Voas https://ieeexplore.ieee.org/document/8405627

[7] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today

[8] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/ oversight/ top-bottom-review/

[9] Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd.

[10] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[11] Vitalik Buterin. (2015). Ethereum White Paper Available at https: //github.com/ethereum/wiki/wiki/White-Paper.

[12] Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. [online] Available at: http://ethdocs.org/en/latest/ introduction/what-is-ethereum.html

[13] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[14] Venkata Naga Rani B, Akshay S, Arun kumar M, Ishwar Kumar M A , (2019) , Decentralized E-Voting System,International Research Journal of Engineering and Technology

[15] Andrew Barnes, Christopher Brake and Thomas Perry. (2016). Digital Voting with the use of Blockchain Technology is Available at https://www. economist.com/sites/default/files/plymouth.pdf

[16] Jonathan Alexander, Steven Landers, and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at https://netvote. io/wp-content/uploads/2018/02/Netvote-WhitePaper-v7.pdf

[17] Jelurida,"Jelurida",2017. Available at: https://www.jelurida.com/sites/ default/files/JeluridaWhitepaper.pdf

[18] Lee, K., James, J.I., Ejeta, T.G., et al.: Electronic voting service using blockchain. J. Digit. Forensics Secur. Law: JDFSL 11(2), 123 (2016)

[19] Jason, P.C., Yuichi, K.: E-voting system based on the bitcoin protocol and blind signatures. Trans. Math. Model. Appl. 10(1), 14–22 (2017)

[20] Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized Oracle Network Available at: https://link.smartcontract.com/ whitepaperMcCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for board room voting with maximum voter privacy. In: International Conference on Financial Cryptography and Data Security, pp. 357–375. Springer (2017)

[21] Dong, Y., Zhang, D., Han, J., et al.: Board electronic voting system based on alliance blockchain. J. Netw. Inf. Secure. (12) (2017)

[22] Wu, Y.: An e-voting system based on blockchain and ring signature. Master, University of Birmingham (2017)

[23] P. Akritidis, Y. Chatzikian, M. Dramitinos,E.Michalopoulos, D. Tsigos, and N. Ventouras, "The vote secure secure internet voting system," in International Conference on Trust Management, vol. 3477. Springer, 2005, pp. 420 – 423.

[24] G. Beroggi, "Secure and easy internet voting," Computer, vol. 41, no. 2, pp. 52 – 6, 2008.

[25] L. Weinstein, "Risks of internet voting," Communications of the ACM, vol. 43, no. 6, pp. 128– 128, 2000.

[26] M. Di Pierro, "What is the blockchain?" Computing in Science &Engineering, vol. 19, no. 5, pp. 92–95, 2017.

[27] Jelurida, "Jelurida", 2017. Available at: https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf