Secure Digital Voting System Analysis and Implementation Using Blockchain Technology

Dr. Priyanka R[1†],

[1] Dept. of Information Science and Engineering, Cambridge Institute of Technology Bangalore, Affiliated to VTU Belagavi (Karnataka), India, priyanka.89.r@gmail.com.

SP Harshini[2†], Sakarapu Jagati[3†],
[2]Dept of Information Science and Engineering, Cambridge Institute of Technology Bangalore,

Abstract

The internet is a crucial factor in how we interact with one another. Creativity and invention have flourished on the internet. Any citizen has the fundamental right to vote, which provides them the ability to choose the nation's future leaders in any democracy. It provides community members with the opportunity to express their opinions. Online voting systems need to be secure and transparent, and blockchain technology has emerged as a possible answer. Online voting systems provide various benefits over traditional voting procedures, including enhanced accessibility, efficiency, and transparency, as digitalization gains in popularity. Blockchain technology offers a decentralized, secure framework for conducting online transactions that makes it difficult for hackers to tamper with the data. Additionally, the use of smart contracts enables the development of open and impermeable voting systems. This article provides a thorough analysis of the advantages and difficulties of blockchain voting systems, including security, transparency, efficiency, usability, and user acceptance. The results of this study indicate that blockchain technology has the potential to revolutionise elections by offering a safe and transparent platform for online voting. To overcome these obstacles and ensure that blockchain voting systems be widely used, further research and development are nonetheless required.

Keywords: electronic voting; security; blockchain-based electronic voting; privacy; blockchain technology; voting; trust

I. Introduction

Today's democracies are built on the consensus that the public achieves via voting. Voting methods using paper have been used since many years. But as the need for digitization grows and online voting technologies emerge, these systems are coming under more and more pressure. Increased accessibility, speed, and openness are just a few benefits that online voting systems have over traditional voting procedures. A promising option for safe and open online voting systems has emerged: blockchain technology.

Many nations today employ the traditional ballot method, which calls for centralized control and an impartial third party to record and tabulate the ballots as well as supervise the voting process. The blockchain is a decentralized and safe distributed ledger system. Blockchain technology provides a foundation for the development of decentralized applications, or dApps, through the use of smart contracts. Smart contracts, also known as self-executing contracts, may be set up to fulfill the needs of a decentralized voting system.

There are various advantages to using blockchain technology in online voting systems. To begin with, blockchain technology offers a safe and impenetrable platform for online transactions, making it challenging for hackers to change the data. Second, because the election's rules and regulations are encoded in the smart contract, using them provides accountability and transparency in the voting process.

This article aims to provide an Ethereum-based voting web application system that provides a secure and open environment for online voting. The suggested method will be accessible to and used by all voters, regardless of their degree of technological expertise.

A)Ethereum Blockchain:

Due to its adaptability and flexibility, Ethereum is regarded as the finest blockchain for decentralized voting applications. Ethereum blockchain is the most famous and widely used blockchain for developing decentralized applications, including voting systems. The need to enforce the rules and regulations of a voting system, Ethereum offers a

decentralized platform in order to build smart contracts.

Voting systems can benefit from the Ethereum blockchain's openness, security, and efficiency, among other features. The use of smart contracts guarantees that the election's laws and regulations are applied in a transparent and tamper-proof way, while the use of a decentralized ledger ensures that the election results are visible and available to all stakeholders. Another significant benefit is the security of the Ethereum blockchain, which is very hard to hack and manipulate.

A sizeable and active developer community that provides a range of tools and resources for building decentralized apps is also present on the Ethereum network. The Ethereum community is continually developing new tools and apps that may be used to increase the functionality and usability of decentralized voting systems.

Furthermore, the Ethereum blockchain allows for the creation of decentralized autonomous organizations (DAOs), which can be used to manage the voting process. DAOs are decentralized organizations that are governed by smart contracts, allowing for a transparent and democratic decision-making process.

Overall, the use of the Ethereum blockchain for voting systems provides several benefits, including transparency, security, efficiency, and accessibility. The large and active developer community, as well as the ability to create DAOs, further enhances the potential of Ethereum for decentralized voting applications.

Benefits of Blockchain-based Online Voting:

Security: Blockchain technology offers a safe online voting platform. Due to the encryption and multiple computer storage of transactions, it is difficult for hackers to change the data.

Transparency: The adoption of blockchain technology has increased the transparency of the election process. All transactions are logged on the ledger, and users may view the election results in real-time.

Efficiency: Blockchain-based online voting platforms may be more effective than traditional voting processes. Results can be attained more quickly due to the quicker process.

Accessibility: For voters who might not be able to physically visit polling places, online voting systems can boost accessibility.

Challenges of Online Voting on Blockchain Technology:

a)Technical Challenges: Some countries would find it challenging to deploy a blockchain-based online voting system since the infrastructure needed to support it could be expensive and the region might not have the necessary technological expertise.

b)User Adoption: Adoption of blockchain-based online voting systems may be gradual due to a lack of awareness, technical knowledge and trust in the technology.

c)Regulation: Implementing blockchain-based online voting systems could present legal and regulatory difficulties. The adoption of blockchain technology in the election process could need changes to the laws and policies already in place.

II. LITERATURE SURVEY

In [1], a self-tallying voting system is suggested that does not need any private channels for voter-to-voter privacy or any trusted third parties for vote aggregating. The suggested protocol requires a lot of computing.

Without using a secret channel or a reliable third party, the authors of [2] suggested a two-round protocol that computes the tally in two rounds. Although the protocol is effective in terms of amputation and bandwidth usage, it isn't always reliable or impartial.

A procedure is suggested by the authors in [3] to enhance the two-round protocol's robustness and fairness (Hao et al., 2010). The authors of [4] propose an E2E verifiable voting system called DRE-ip (DRE-i with increased privacy), which gets around DRE-i's drawbacks. DRE-ip encrypts the vote live during voting rather than pre-calculating ciphertexts. DRE-IP provides a substantially greater privacy guarantee than DRE-i while still achieving E2E verifiability without TAs. The Mixnet protocol in [4] achieves end-to-end verifiability by recovering the plaintext ballot in an unfavorable way by generating the ciphertext over a network of mix servers. To achieve end-to-end (E2E) verifiability, Scantegrity is proposed in[5],

which uses confirmation codes to let voters to verify to themselves that their votes are included in the final total as they truly are.

Another voting method, called Prêt à Voter, is put up in [6] and preserves voter anonymity by creating a ballot with two columns, one for the voter's decision and the other for the voting possibilities. The research in [7] is based on Prêt à Voter, but it employs homomorphic tabulation and scratch stripes to enable off-line audits of ballots. Bingo Voting [8, 9] is one of the several ways for electronic voting that has been suggested.

EXISTING SYSTEM:

The current electoral system is operated manually. Since the voter must physically travel to many polling sites to cast their ballot, time is lost. This prevents many individuals from voting, which is one of the most significant and worrying factors. Each and every vote matters in a democracy. A new online system that limits vote frauds and increases voting efficiency and transparency can take the place of the current traditional voting system.

Existing System Drawbacks:

There are a number of issues with current online voting methods that prevent widespread acceptance and efficacy. Some of the major negatives include:

1. **Anonymous voting**: After a vote is cast via the system, which may or may not include a choice for each candidate, it should remain anonymous to everyone, including the system administrators.
2. **Individualized ballot procedures**: It's still up for debate how votes are represented in the databases or web applications involved. A hashed token is more likely to provide obscurity and integrity than a transparent text message, which is the worst possible strategy. In the meanwhile, the vote should be disreputable because it cannot be secured by the symbolic resolution.
3. **Verifiability of ballots by the voter (and only by the voter):** The voter must be prepared to see and verify his vote during voting. This is often critical to identify in order to avoid or at least be aware of potentially harmful activity. Apart from providing irrefutable evidence, this counter can certainly boost voter confidence. In some recent applications, the region unit partially solves these problems itself. However, it suggests that electronic voting is currently used in many countries, including Brazil, Great Britain, Japan, and the Republic of Estonia. The Republic of Estonia should be judged differently than others because they offer a full electronic voting decision, which is said to be equivalent to ancient paper elections.
4. **High initial setup costs:** Although online polling systems are much cheaper to operate and maintain than traditional polls, the initial setup can be expensive, especially for businesses.
5. **Growing security concerns:** Cyber attacks pose an outstanding threat to the public. No one would be satisfied with the responsibility if a hacking attempt is successful during the election. DDoS attacks are documented and mostly false in elections. The US Civilian Immunity Commission recently released a report on the state of North American state elections. That's right; Ronald Rivest clearly stated that "hackers have countless ways to use offensive extraction machines".
6. **Security**: The security of online voting systems is susceptible to hacking and other cyber-attacks that might jeopardize the results. Malicious actors have the ability to alter vote data, alter election results, or attack the system with a denial-of-service assault.

7. **Privacy:** Internet voting systems may compromise voter privacy because their personal information and voting choices may be accessible to unauthorized individuals or organizations. This can lead to voter intimidation or discrimination, which can undermine the integrity and legitimacy of elections.

8. **Accessibility:** All voters may not be able to use online voting methods, particularly those who lack computer literacy, lack Internet connection or have impairments. As a result, some voter groups may not be represented or participate as expected, which might compromise the democratic foundations of elections.

9. **Verification:** Online voting systems may not provide a transparent and verifiable process for voters to confirm that their vote was correctly cast and counted. This can lead to mistrust of the election results and weaken the legitimacy of the results. 10. Costs. Developing and maintaining online voting systems can be expensive and require significant resources and infrastructure. This may limit the adoption of online voting systems, especially in lower-income or developing countries.

These drawbacks have led to a lack of trust in existing online voting systems, and have hindered their widespread adoption. Addressing these challenges is crucial for the development of effective and secure online voting systems.

Objectives:

Thus, the voting system that is hereby conceived must satisfy the following requirements:

1. The electoral process must be transparent and open to public scrutiny.
2. The election process must make sure that the voter's choice is noted.
3. Voting is only open to qualified citizens.
4. The election process must guard against fraud.
5. No organization with a desire for power should be allowed to influence and rig elections.

When using a blockchain, the most important requirements are met:

• **Authentication:** Only people who are registered to vote may do so.
• **Anonymity:** The mechanism shields the identities of voters from the votes they cast.
• **Accuracy:** Votes cast are recorded forever and cannot be altered or amended in any way.
• **Verifiability:** A vote tally may be used to confirm the system.

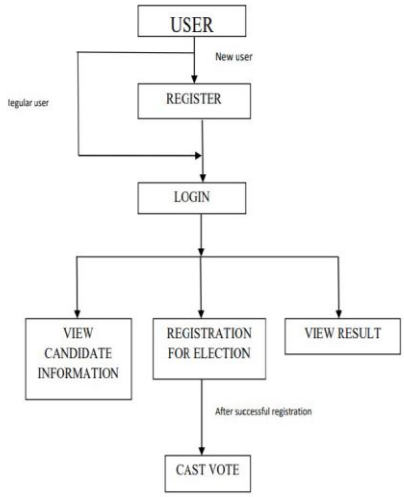
III. PROPOSED SYSTEM

The current electoral system needs improvement due to the aforementioned factors. This can be accomplished by switching to a new system that will reduce voting fraud and improve voting and counting efficiency in place of the current one.

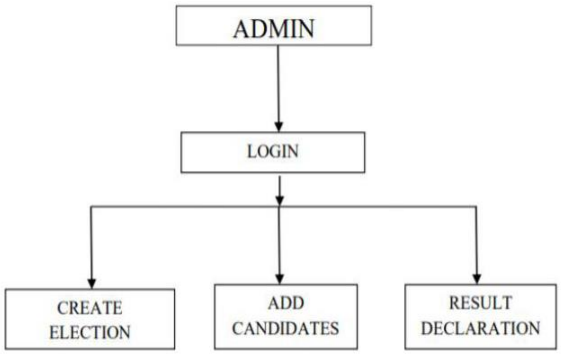
1. User registration, user login, and admin login are all features of the online election system.
2. Voters can log in and exercise their right to vote using this online voting system, which manages voter information.
3. During registration, the voter is asked the following: Full name, age, Aadhaar card number, mobile number. email address and after confirmation access rights are granted.
4. The voter would be required to input his Aadhaar ID in order to cast his ballot. Once the voter has been verified, they are then able to select a candidate from the list. In an election, a voter may only cast one vote for each candidate.
5. Users of the software can log into their profiles and upload all of their data, including prior milestones, to the system. The administrator has access to each candidate's information.

6. The software system also allows voters to see the list of candidates in their region. The system administrator has general system rights and can control and delete all information that is not related to selection rules.

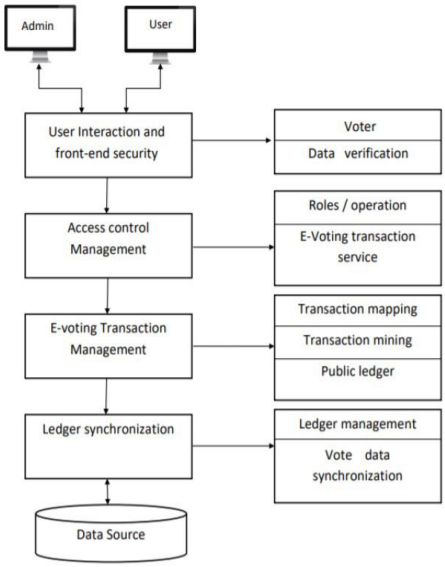
USER FLOWCHART DIAGRAM :



ADMIN FLOWCHART DIAGRAM :



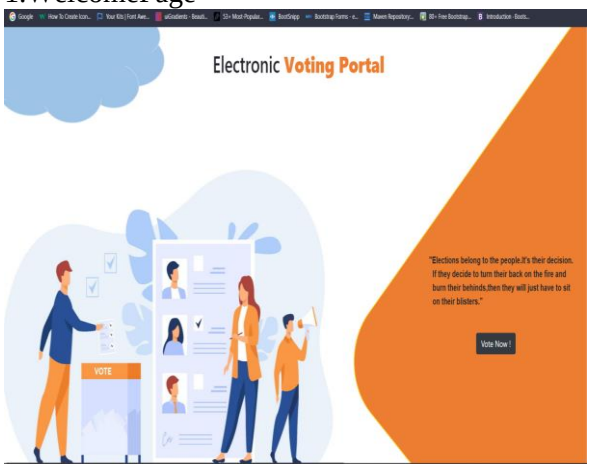
IV. METHODOLOGY AND IMPLEMENTATION



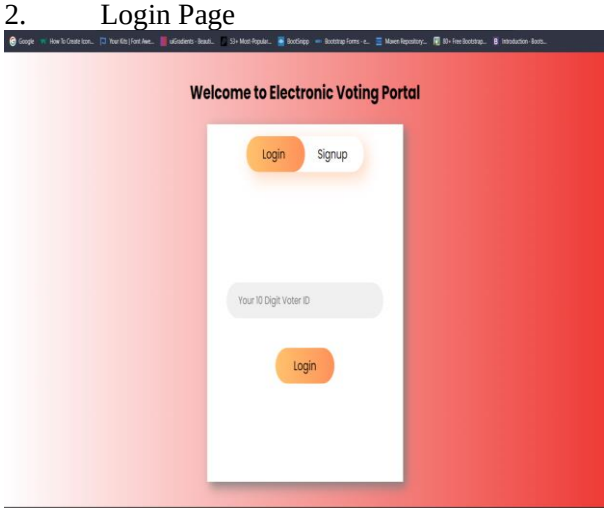
Tools and Technology:

1. Ethereum Blockchain
2. Web3.js
3. Truffle
4. Ganache
5. Metamask
6. Solidity Programming Language: smart Contract
7. HTML, CSS, Javascript, jsp, node, MySQL

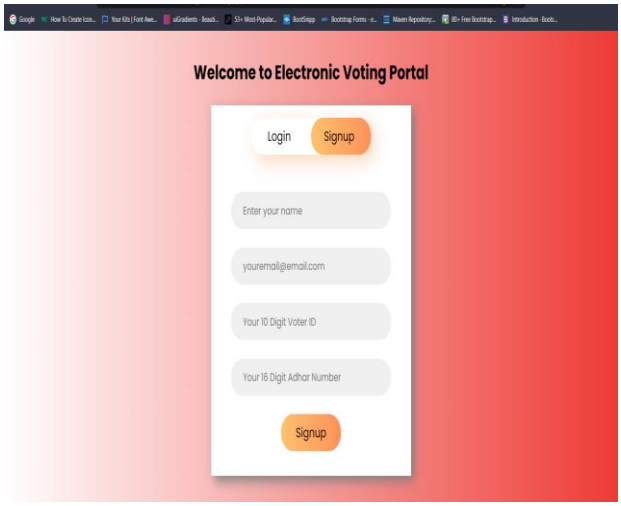
1.WelcomePage



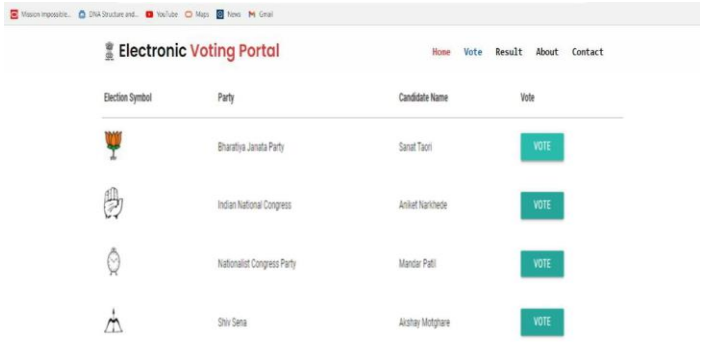
2. Login Page



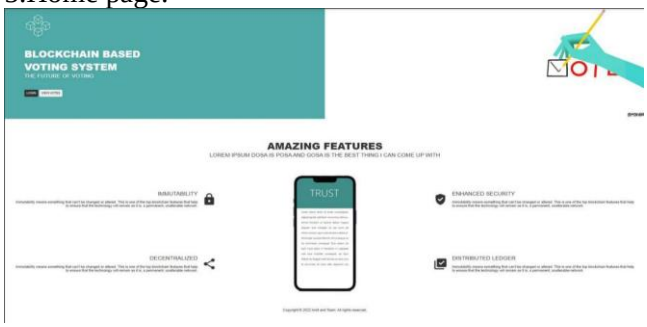
3. Sign-up Page



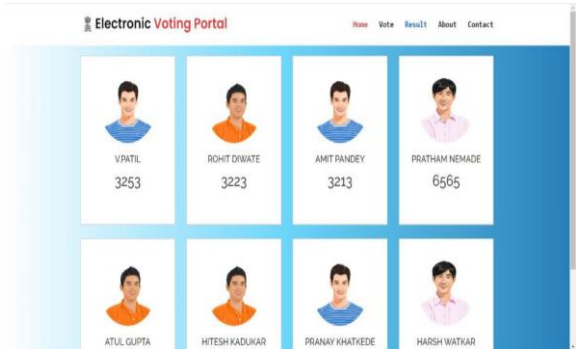
4. Voting Poll:



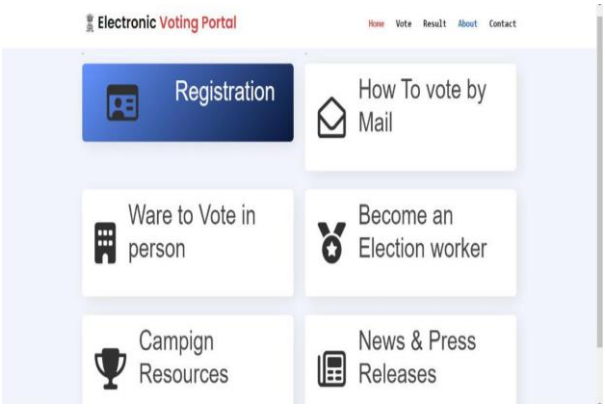
5.Home page:



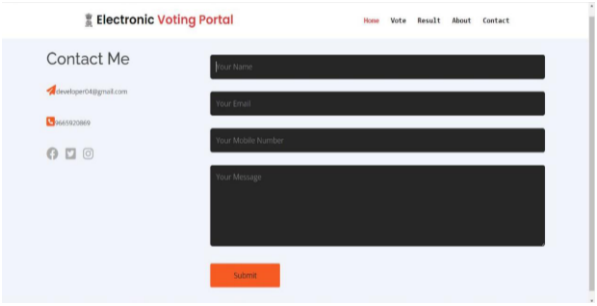
6.Result:



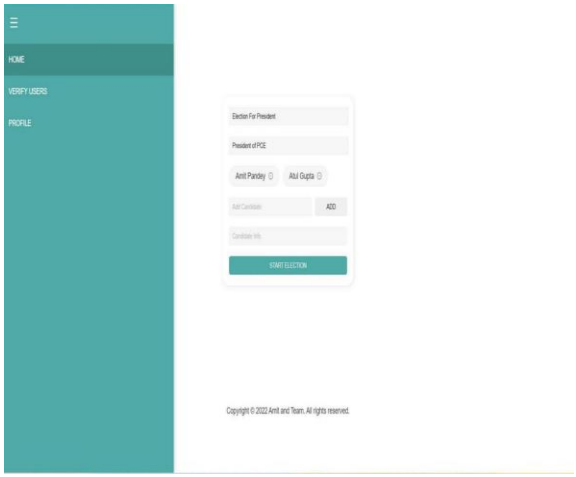
7.About:



8.Contact us:



9.Admin Panel:



V. CONCLUSION

The creation of accessible, safe, and transparent online voting systems is made possible by the use of blockchain technology. Voting systems can be developed to guarantee the accuracy and transparency of the electoral process by utilising the decentralized and tamper-proof properties of blockchain technology.

Smart contracts are used in blockchain voting systems to enable the development of transparent, tamper-proof rules and regulations for the election as well as the automatic and correct recording of the results. Voters can confirm that their votes have been correctly counted, and election officials may audit and verify the election results thanks to the transparency and immutability of the blockchain.

Blockchain voting methods provide a lot of benefits., even though there are still issues to be solved, such as the requirement for widespread adoption and addressing security issues. Blockchain technology has the ability to transform the electoral process and reinforce the foundations of democracy by providing a more safe, open, and accessible platform for online voting. Blockchain-based voting systems are anticipated to become more widespread in the near future as more study and development are done to improve them.

VI. REFERENCES:

1. Kirillov, Denis, Vladimir Korkhov, Vadim Petrunin, Mikhail Makarov, Ildar M. Khamitov, and Victor Dostov. ”Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain.” In International Conference on Computational Science and Its Applications, pp. 509-521. Springer, Cham, 2019.

2. Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. ”Large-scale election based on blockchain.” Procedia Computer Science 129 (2018): 234-237

3. Moura, Teogenes, and Alexandre Gomes. ”Blockchain voting and its effects on election transparency and voter confidence.” In Proceedings of the 18th Annual International Conference on Digital Government Research, pp. 574-575. ACM, 2017.

4. ”Blockchain Tutorial.” Weka, Solidity, Org.Json, AWS QuickSight, JSON.Simple, Jackson Annotations, Passay, Boon, MuleSoft, Nagios, Matplotlib, Java NIO, PyTorch, SLF4J, Parallax Scrolling, Java Cryptography. Accessed September 11, 2019. https://www.tutorialspoint.com/blockchain/index.html

5. Barnes, Andrew, Christopher Brake, and Thomas Perry. ”Digital Voting with the use of Blockchain Technology.” Plymouth University. Accessed Dezembro 15 (2016): 2017.

6. Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis. ”EVoting with blockchain: an E-Voting protocol with decentralisation and voter privacy.” In 2018 IEEE Inter- national Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561-1567. IEEE, 2018.

7. Ayed, Ahmed Ben. ”A conceptual secure blockchainbased electronic voting system.” International Journal of Network Security & Its Appli- cations 9, no. 3 (2017): 01-09.

8. Liu, Yi, and Qi Wang. ”An E-voting Protocol Based on Blockchain.” IACR Cryptology ePrint Archive 2017 (2017): 1043.

9. Yu, Bin, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. ”Platform-independent secure blockchain-based voting system.” In International Conference on Information Security, pp. 369-386. Springer, Cham, 2018.