International Journal of Innovative Science and Modern Engineering (IJISME)
ISSN: 2319-6386 (Online), Volume-11 Issue-7, July 2023

Blockchain-Based E-Voting System

Ajay Kumar Yadav, Hari Om Patel, Shivam Kumar

Abstract: ***To elect the most qualified candidate, every democracy needs an open voting procedure that meets the needs of the people. The current voting procedures, however, have serious weaknesses and lack security and transparency. This survey research looks at the possible uses of BC technology in e-voting systems to improve the voting process and solve the issues of restlessness, privacy, and security. This study tries to evaluate several distributed electronic voting system implementations based on blockchain technology. While some have just existed as drafting papers, others have been implemented in the real world. An electronic voting system built on blockchain improves security and privacy while significantly lowering expenses. By outlining a case study involving the conduct of an election and the adoption of a blockchain-based application that increases security and decreases the cost of organizing a national election, we evaluate the potential of distributed ledger technology.***

Keywords: Privacy, Blockchains, Security, Electronic Voting, Information Technology.

I. INTRODUCTION

In recent times, there has been a growing concern regarding government mistrust and external interference in the electoral processes of various nations. These issues have raised critical concerns that surpass anything experienced in the past. The right to vote and choose representatives is a fundamental democratic principle, and disregarding or violating this right poses a significant problem. The establishment of fair and transparent elections is crucial for upholding the freedoms enjoyed by the majority of people today. In every nation, voting is a serious occasion that has great significance. Due to their centralized form, traditional paper-based elections have several flaws in terms of security, privacy, fraud, integrity, and fairness. Although attempts have been made to switch to online voting methods, most of these worries have not been properly addressed. However, the investigation of novel approaches or technologies that might lessen or repair these shortcomings has been stimulated by this circumstance. Blockchain is a decentralized and transparent public ledger that offers several distinct characteristics. These features can be summarized as follows:

Manuscript received on 04 June 2023 | Revised Manuscript received on 14 July 2023 | Manuscript Accepted on 15 July 2023 | Manuscript published on 30 July 2023.
*Correspondence Author(s)
Ajay Kumar Yadav, Department of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: 7355201716ajay@gmail.com, ORCID ID: 0009-0005-0293-4135
Hari Om Patel*, Department of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: hariompatel3369@gmail.com, ORCID ID: 0009-0009-9349-3986
Shivam Kumar, Department of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: shivam.20scse1010405@galgotiasuniversity.edu.in

Distributed: The ledger is maintained and validated by a network of computers, or "nodes," that operate the blockchain. This decentralized strategy prevents data from being stored in a single location and does away with the necessity for a central authority.

Immutable: Once data is recorded on the blockchain, it becomes incredibly difficult, if not impossible, to alter or tamper with. Information is organized into blocks, with each block containing a unique hash identifier. Modifying a block would require changing subsequent blocks, making any tampering evident and impractical.

Transparent: Transparency is a core aspect of the system. Every transaction and modification made to the ledger is visible to all participants. This transparency promotes accountability and enables auditing and verification by anyone who has access to the applications.

Blockchain technology holds great promise for many applications outside of cryptocurrency due to these specific properties. The safe, decentralized, and transparent characteristics of blockchain can be advantageous to sectors including supply chain management, voting systems, and smart contracts. Its capacity to enable safe transactions while obviating the need for middlemen gives it the potential to revolutionize several industries.

II. LITERATURE SURVEY

Several studies have explored the implementation of blockchain technology in e-voting systems to address security and privacy concerns. The privacy, integrity, security, and high costs of traditional paper ballot methods were emphasized in one study [1]. They put out a framework for enhancing the electronic voting system using blockchain, especially Ethereum and smart contracts. Through the Truffle framework, Ethereum and smart contracts provided testing and verification, while Meta-mask, a Google extension, allowed communication with Ethereum nodes.

A blockchain-based electronic voting system was built by researchers [2] using double-envelope encryption. Voter participation, electoral commissions, and the blockchain network made up the system's three parts. They made use of the distributed ledger function of blockchain to guarantee availability, and the hash function of blockchain was used to improve the security and verifiability of the system. Even in the face of attacks, the system-maintained availability and resolved coercive concerns. However, due to the electoral commission's substantial dependence on key generators, questions were raised concerning source centralization. Further research is needed in the areas of potential blockchain advancements and standardized blockchain protocols.

A leveled structure blockchain-based electronic voting system was suggested in research [3].

The system connected each level to the one above it, ensuring consistency, privacy, speed, and security. To avoid latency problems in district-based voting, nodes at the lowest level included human computers and voting locations. Furthermore, a research study [4] suggested a Blockchain as a Service (BaaS) method for establishing an e-voting system. The authors utilized smart contracts to create legitimacy for both voters and the voting process. The blockchain network was set up using Go-Ethereum authorization and Proof-of-Authority (POA) as a private network, boosting security, and eliminating coerced voting. The smart contract contained role descriptions, agreements relating to the election process, and transactions.

Bronco Vote is a different blockchain-based voting method that was suggested in [5]. The blockchain of Ethereum, smart contracts, and homomorphic encryption were all used in this system. The creator, the register, and the voting entities were its three constituent parts. The framework was created to be simple to implement while still guaranteeing control and confidence in the process.

In a separate paper [6], a technique was presented that employed hash values for securely recording vote results. The system utilized blockchain technology like the Bitcoin system, focusing on database recording. Each node created a private and public key before the election, and public keys were shared among all nodes. After the election, nodes produced blocks and performed verification to update the database. Digital signatures were employed for dependability, and turn rules were devised to prevent collisions and ensure blockchain integrity.

These studies demonstrate how blockchain technology may be used to address security and privacy issues in e-voting systems, exhibiting various methods and features to enhance the procedure.

III. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

In this section, we first go through the design elements that must be considered while developing an electronic voting system. Then, we provide an overview of blockchain and smart contract technology as a service for the construction of electronic voting systems.

A. Design Considerations

We have created the following list of requirements for a workable e-voting system after carefully examining current e-voting technologies and the conditions essential for their effective deployment in a national election: (i) The electoral process shall prohibit coercive or compelled voting. (ii) An identity verification service shall be used as a secure authentication technique for the electoral system. (iii) The electoral process ought to make sure that votes cannot be linked to specific electors. (iv) The electoral process must be transparent, guaranteeing that each voter obtains independent verification that their vote was correctly counted without jeopardizing their privacy. (v) The electoral process should include safeguards against any vote-rigging or third-party influence. (vi) The voting process and election results should not be under the control of any one body due to the election system. (vii) Only those who are eligible should be able to vote under the electoral system.

IV. ANALYSIS

Blockchain-based apps can be created using web3 technologies. The most widely used blockchain frameworks are R3 Corda, Hyperledger, Ethereum, and Bitcoin. We look for a computer that will analyze the content of particular articles the best. However, we discovered that the literature often lacks information on general terms and conditions of use. The overall idea of blockchain-based electronic voting and related challenges have been covered in several studies. It appears that everyone agrees that blockchain-based technology can be applied to electronic voting. He did not, however, go into great depth about the usage or directions. But, according to studies, the chart shows how the dispersion of blockchain-based platforms is used.

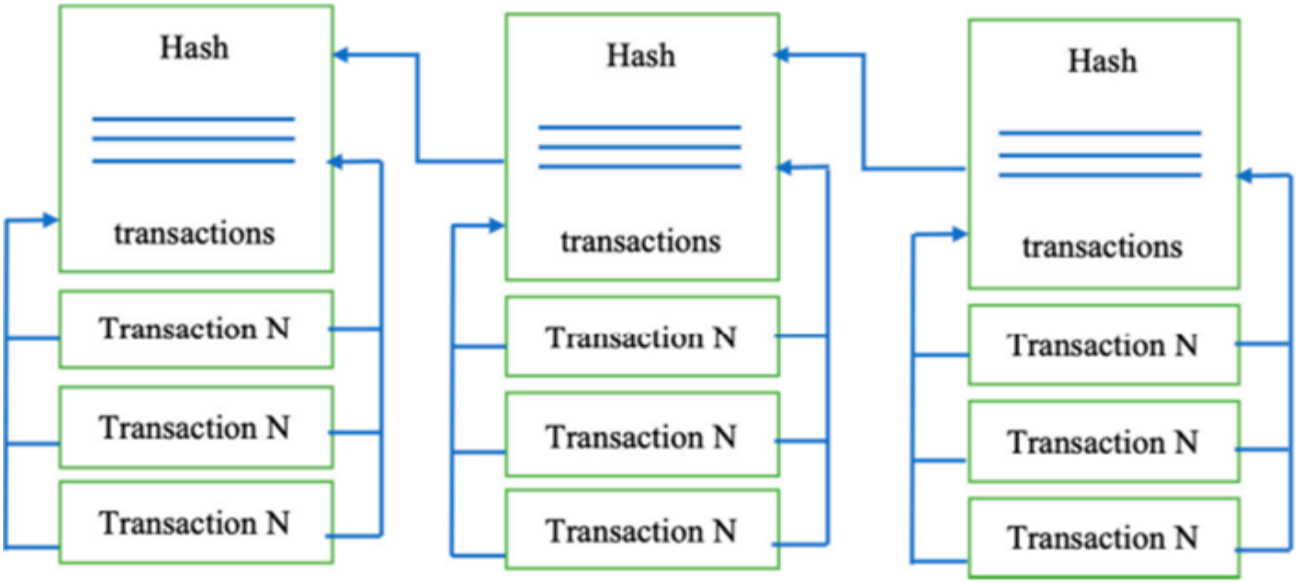

Fig.1 Dispersion of Blockchain-Based Platforms

A. Proposed Approach:

For our study plan, there are two models we intend to complete at our level. The two modules of are as follows:

1. Front-end implementation
2. Back-end uses Solidity to use blockchain.

Each of these models will be considered a phase, and later phases will include integration and testing of these models.

Stage 1: In this stage, we will introduce the front-end module, where we will create an interactive UI for administrators and users. At the same time, research studies on using blockchain in equity applications will be completed.

Stage 2: In this stage, we will introduce the backend module, implement the blockchain using the Ethereum framework, and transform the system into a distributed system. was used.

Stage 3: Integration of two variables and testing of the platform will be done at this stage.

B. Model:

A blockchain may be easily explained by seeing it as a collection of interconnected blocks. Each block serves as a container for data and is compiled into the overall structure known as the superblock through a process called "mining". Verification of each block can be achieved using a unique hash value, also known as a digital fingerprint. Additionally, each block may contain the hash of the previous block, creating a sequential chain starting from the initial block, known as the genesis block. Through this model, all files within the system can be linked together using their respective hash values.

C. Detailed Design:

The project's flow is explained from both the user end and the back end in the use case diagram that follows.

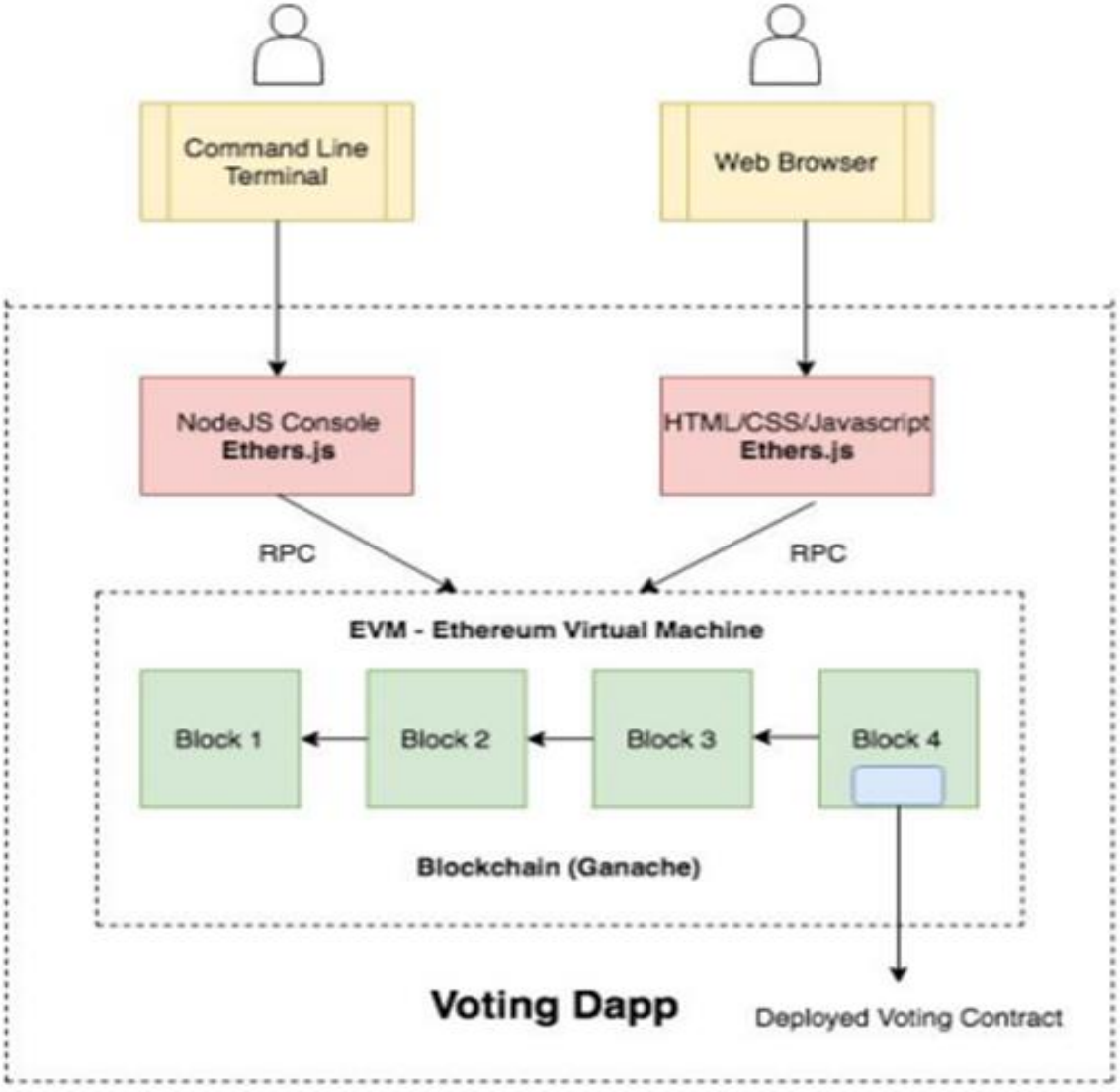

Fig.2 User end and the back end in the use case diagram

D. Use Case Diagram:

To begin the voting process, users are required to register on the website. Once registered, users can proceed to the voting page, where they will enter the One-Time Password (OTP) received via email from the address blockchainev@gmail.com. Upon successful entry of the OTP, users will gain access to cast their votes. After casting a vote, users will receive an acknowledgment prompt confirming their successful participation. Finally, users can choose to log out after completing the voting process.

E. Methodology/Procedures (Approach to solve the problem)

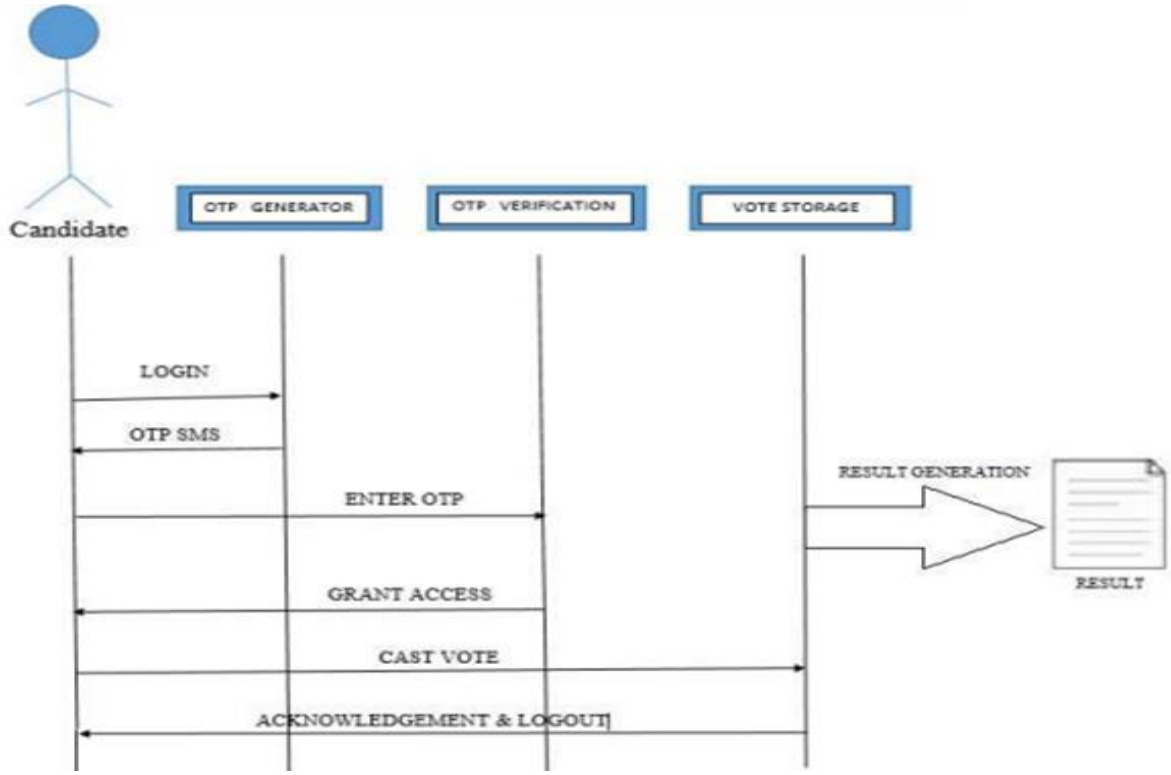

Fig.3 Approach to solving the problem

V. CONCLUSION AND FUTURE WORK

Establishing trust in e-voting systems is crucial for minimizing fraud in the election process. This survey highlights the significance of utilizing blockchain technology to address this issue and ensure transparency throughout the entire process. Previous studies have revealed that lots of Ethereum-based e-voting systems lacked a consensus mechanism based on application, roles, and stakeholders. Additionally, the existing body of related work failed to provide sufficient motivation for managing and maintaining the blockchain. To provide an overview of the frameworks employed, achievements made, and areas that require improvement, a summary table comprising eight papers have been presented, offering insights for future enhancements.

SCOPE

The system can be improved by implementing the following enhancements:

- Introducing an Aadhar number verification system for added authenticity.
- Establishing a connection between the application and Government voting system data for more accurate information.
- Strengthening security measures to ensure the system's integrity and protect against unauthorized access.
- Enhancing the Graphical User Interface (GUI) of the application to improve user experience.
- Incorporating local languages to cater to the needs of individuals residing in rural areas and those with limited education.
- Including information about a candidate's previous social work and qualifications to assist voters in making informed choices.
- Implementing a suggestion system that allows the public to provide feedback and suggestions to the elected candidates.
- Integrating a complaint system that enables citizens to file complaints against any candidate for proper investigation and action.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Bell, S., Benaloh, J., Byrne, M. D., DE Beauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A secure, transparent, auditable, and reliable voting system.", in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.
2. 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.
3. Adida, B.; 'Helios (2008). "Web-based open-audit voting.", in Proceeding of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.

4. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-variable optical scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008. [CrossRef]
5. Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "Bingo voting: Secure and coercion- free voting using a trusted random number generator.", in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124. [CrossRef]
6. Adida B. and Rivest, R. L. (2006). "Scratch and vote: Self-contained paper-based cryptographic voting.", in Proceeding of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40. [CrossRef]

AUTHORS PROFILE

Hari om Patel I am an enthusiastic student continuing my academic journey in computer science. I have a deep curiosity and passion for deep learning and I am dedicated to expanding my knowledge in the field. I am currently enrolled at Galgotias University studying B.tech in Computer Science. I actively participate in various academic activities and research projects related to ML, Data science, etc. Through writing, my goal is to share insights and perspectives on projects and contribute to the ongoing discourse in this field. I believe in the power of effective communication and strive to communicate complex ideas in a clear and accessible way. As a student, I bring a new perspective and desire to learn. I actively seek opportunities to collaborate with peers and experts in the field, creating a dynamic and enriching learning environment.

Ajay Kumar Yadav I am currently enrolled at Galgotias University studying B.tech in Computer Science. I actively participate in various academic activities and research projects related to ML, Data science, etc. Through writing, my goal is to share insights and perspectives on projects and contribute to the ongoing discourse in this field. I believe in the power of effective communication and strive to communicate complex ideas in a clear and accessible way. As a student, I bring a new perspective and desire to learn. I actively seek opportunities to collaborate with peers and experts in the field, creating a dynamic and enriching learning environment. With a keen interest in ML, Data Science, and blockchain, I research the latest developments and new trends and stay informed on Blockchain advancements. Committed to personal growth and development, I am constantly improving her writing skills and expanding my professional knowledge. I am excited about the opportunity to share my knowledge and insights with readers while learning from the experiences and perspectives of others in the industry. He is driven by a desire to make a positive impact and contribute to the academic and intellectual community.

Shivam Kumar I am an enthusiastic student continuing my academic journey in computer science. I have a deep curiosity and passion for deep learning and I am dedicated to expanding my knowledge in the field. I am currently enrolled at Galgotias University studying B.Tech in Computer Science. I have a good grasp of programming concepts, data structures, and algorithms, and be able to translate ideas into functional code. strong communication skills, allowing them to express their ideas clearly, actively participate in group discussions, and work effectively in a team environment. I have strong time management and organizational skills, allowing me to prioritize tasks, meet deadlines, and effectively manage my workload. I enjoy exploring new concepts, coding, and problem-solving. Their enthusiasm drives their commitment to continuous learning and improvement.