Enhancing Trust and Transparency with Blockchain-Powered Remote Electronic Voting

Sushil Kumar
DSDL, Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
drsushil.cs@gmail.com

Shubham Verma
Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
shubhamverma2258@gmail.com

Shaurya Gupta
Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
thats.shaurya@gmail.com

Shivam Shrivas
Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
shivambundela021@gmail.com

Vimal Kumar Dubey
Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
vimalkumardubey23@gmail.com

Umang Rastogi
Computer Science and Engineering
KIET Groups of Institutions, Delhi-NCR
Ghaziabad-201206, Uttar Pradesh, India
rastogi225103@gmail.com

***Abstract*—The inconvenient nature of making the conventional, physical trip to the polls has been blamed for the rise in voter disinterest in elections. Remote electronic voting, or "e-voting" appears to be a promising remedy. In addition to offering quicker results, electronic voting also solves practical issues, which may boost voter turnout. However, to foster confidence in the democratic process, e-voting needs to meet strict requirements for security, dependability, and openness. Scholarly research explores different approaches to distant electronic voting, with an emphasis on using blockchain technology. The decentralized structure of blockchain eliminates the need for reliable middlemen and allows for safe and transparent transactions. Blockchain improves voting process integrity by guaranteeing transparent data storage, offering tamper-resistant and verifiable. Furthermore, the electoral process can be further streamlined by introducing automated agreements between users through the integration of smart contracts into blockchain technology. Blockchain technology is being used in electronic voting systems to improve security and transparency while also addressing issues with trust in the digital voting environment. Blockchain presents a potential paradigm change in the design and implementation of remote electronic voting systems, removing the need for centralized authorities and introducing features like smart contracts. This might lead to a more transparent, safe, and reliable democratic process.**

***Index Terms*—Decentralization, Ethereum, Security, Smart Contracts, Voting System**

I. Introduction

Due to the inherent hardship of traveling to actual polling places, the boom in interest in remote electronic voting, or e-voting, has shown to have a paradoxical effect on voter participation. At the same time, it has increased involvement and contributed to higher rates of abstention. Acknowledging this difficulty, it is imperative to reexamine current voting procedures to improve election accessibility and transparency. Investigating blockchain technology, which has surfaced as a viable means of supporting electronic voting systems, is one encouraging path toward accomplishing this aim.

Blockchain offers a strong foundation for changing the face of electronic voting, even if it was first created for Bitcoin transactions [1], [2]. Blockchain addresses the complexity of online voting, which is frequently difficult for citizens to audit and verify. Blockchain is decentralized, safe, and anonymous [3]. In contrast to conventional voting methods, which inherently depend on a Trusted Third Party (TTP), blockchain technology does away with the necessity for these middlemen, promoting an atmosphere devoid of trust for the flow of information [4]. This change is especially important when it comes to electronic voting because maintaining the integrity of the democratic process depends heavily on confidence.

This study expands on our knowledge of blockchain-based electronic voting solutions by conducting a thorough review of important systems. The goal of this investigation is to shed light on potential future developments for distant electronic voting systems that could improve security, transparency, and trust in the democratic process. The study intends to make a significant contribution to the continuing conversation about the development of electoral systems by exploring the nuances of blockchain technology concerning voting. It aims to clarify the possible routes for incorporating blockchain technology into election processes by careful examination and contrast, with a focus on promoting accountability, diversity, and resilience within the democratic system [5]. The main objective of this study is to provide a comprehensive knowledge of how blockchain technology may affect electronic voting. Furthermore, the article seeks to further the development of more safe, transparent, and reliable election procedures by investigating possible directions for the creation of distant electronic voting systems. In the end, this research aims to pave the way for the successful integration of emerging technologies into the democratic governance framework, thereby strengthening the foundations of democracy and enhancing citizen participation in the process through its thorough examination of blockchain-based electronic voting solutions.

II. Related Work

This segment offers a foundational review of prior studies that delved into the scalability of blockchain technology for electronic voting. The investigation involved utilizing digital repositories like IEEE Xplore Digital Library, Scopus, ScienceDirect, SpringerLink, and ACM Digital Library to locate and assess existing literature systematically. This approach enabled a meticulous examination and analysis of the endeavors undertaken in this field.

A multi-layered blockchain system that relies on voting and its token for transactions [6]. It is connected to the Bitcoin blockchain by Skipchain, which provides immutability. It was utilized in the 2018 presidential election in Sierra Leone. A Secure and Optimally efficient Multi-Authority Election Scheme [7] suggested a voting mechanism for private, secure, and effective computerized voting. While there is great potential for large-scale voting, these projects do not have the same protections as voting on PCs and allow similar control to the Ethereum version. A confidential, anonymous, transparent electronic election suitable for mass electronic elections where trust among participants is low is proposed [8]. However, since there is no third-party authority to perform post-election audits, their systems cannot prevent DoS attacks [9]. The use of a signature ring protects voter privacy but creates problems in managing multiple signatories. A blockchain-based electronic voting scheme (BES) is launched to use blockchain technology to improve the security of electronic voting in a peer-to-peer network [10]. BES is based on blockchain technology. The challenge of countermeasures required the involvement of a responsible third party. Although particularly suitable for decentralized use in systems with large numbers of agents, decentralized systems [11] with large numbers of secure computers can lead to higher computational costs, especially when dealing with complex calculations and large numbers of participants [12].

A novel electronic voting method called scantegrity emphasizes end-to-end verification via authentication codes [13]. This approach increases transparency and trust by allowing voters to verify their votes throughout the process. Overall, it provides a solution for security and transparency in electronic voting. A self-voting system was proposed that does not rely on a trusted third party or private property for voting to protect voters' privacy [14]. The system highlights the lack of trust and morality to ensure freedom without compromising justice. The innovation of this system is that it offers a distributed, secure, and privacy-controlled voting solution. A two-stage vote counting system in electronic voting was proposed that eliminates the need for proprietary or trusted third parties [15]. The process supports a decentralized approach, emphasizing efficiency in computing and bandwidth usage. Despite its advantages, the process involves a balance between efficiency and fairness, making it suitable for specific voting contexts. An end-to-end voting system was introduced that overcomes the limitations found in its predecessor [16]. The system will be designed with usability in mind, providing access to various components. The potential impact of this system is to lead to advancements in electronic voting security by striking a balance between authentication, privacy, and usability.

An online voting leadership method based on the Ethereum blockchain, with self-accounting, and using open voting, an electronic voting method, as a benchmark [17]. The system uses blockchain technology to increase transparency, security, and trust in the voting process. Smart contracts using Ethereum can enforce and manage voting rights, ensuring fairness without the need for an intermediary. This study addresses potential challenges with blockchain and highlights usability and accessibility.

A vote of confidence was proposed in the Ethereum blockchain [18]. It leverages the Ethereum Virtual Machine to ensure data integrity and transparency and gives every phone one vote in every election. The research conducted which examines blockchain-based electronic voting systems [19]. This discussed about the use of blockchain to protect database management in electronic voting, suggests AES encryption of fingerprint data, and focuses on the security of voting at different polling stations. A secure electronic voting was proposed based on blockchain, where authentication, anonymity, accuracy, and proof are essential. The system encourages mobility, flexibility, and efficiency [20]. However, the system assumes voters are using security tools, which opens up the potential for security if it is compromised. Aadhar cards and fingerprint authentication should be used for safe electronic voting in India [21]. The system allows voters to vote online by using their fingerprints to identify voters at the ballot box. Relying electronic voting was proposed using blockchain technology [22]. The system uses a security hashing method to ensure data security and expose the details of block creation and block binding. The principle of blockchain optimizes the blockchain to meet the requirements of the voting process. A security assessment of Indian voting machines was conducted [23]. According to anonymous sources, the research reveals flaws in electronic voting machines (EVMs). This shows that EVMs are vulnerable to mass attacks that could alter the results and compromise the secrecy of the vote. Map two attacks using custom hardware. The integrity proof of this BSJC seeks to be a dependable electronic voting system that addresses the issues of security, privacy, and anonymity in elections [24]. However, challenges include complex math and proof-of-work work, as well as concerns about collaborating with others; This can lead to data breaches, leaks, and unfair outcomes. Additionally, the construction and sealing of larger blocks will also delay the election [25].

III. Proposed Methodology

To build a strong online voting system powered by blockchain technology, the proposed methodology represents a systematic approach. This research opens with an unequivocal explanation of its aims, which revolve around boosting openness, security, and accessibility inside the political process while simultaneously resolving the issues ailing online voting systems. An extensive literature evaluation is a crucial component of the process since it provides the framework for research. This paper includes a thorough investigation of previous research in the fields of blockchain technology and online voting. It serves a variety of purposes, including providing us with deep insights into previous research, identifying gaps and deficiencies in the corpus of current knowledge, and providing us with up-to-date information on the most recent trends and advancements in this rapidly evolving subject. Equipped with this understanding, set out to delineate the exact specifications, both functional and non-functional, that the online voting system needs to meet. These exacting specifications serve as the architectural blueprints that direct research in the ensuing stages. After establishing the system's organizational structure, begin the complex process of gathering and preparing data. The gathering of various datasets, including voter data, voting records, and blockchain-related data, is what defines this phase. Since the quality of the data have at their disposal determines the integrity of research, it becomes critical to ensure that the data is accurate, reliable, and suitable for analysis.

The proposed methodology places a high priority on system security, which leads to a thorough security study. This phase identifies possible risks, threats, and vulnerabilities related to the online voting system. To strengthen the system's defenses and maintain the integrity of voter data and the electoral process, mitigation techniques are put forth. This study is also infused with ethical considerations, with particular attention paid to privacy, data security, and the concepts of justice and equity in the voting process. These ethical principles must be upheld, and the proposed methodology carefully describes the actions done to make sure the research complies with ethical standards and laws. As the end of this study journey draws near, the phase of outcomes and data analysis becomes more apparent. Research findings from data analysis, security analysis, and user testing are presented at this stage. By utilizing a combination of statistical and qualitative techniques, they uncover information on functionality and security, taking into account the issues with India's current electoral system, like long voting lines, vote rigging, booth capturing, etc. The goal is to completely eradicate these issues and implement transparency and authenticity into the voting process. Verifying that the person casting a ballot is a legitimate candidate is necessary. Accomplish this by utilizing a one-time password (OTP) and authenticating the person's Aadhar data.

It is originally intended for the voter to register on the application. The database will be used to store these details. He needs to log in with the information he gave when signing up to cast his vote. He will receive a generated OTP on his mobile device. He is directed to the voting portal to cast his ballot after being confirmed. The user cannot log in again after logging in since his data is entered into the database. The application ensures that the user can only vote for one candidate at a time after being redirected to the voting portal. According to the system design of this infrastructure, the user must first register with the application before logging in; the application handles other requirements like login without registering and

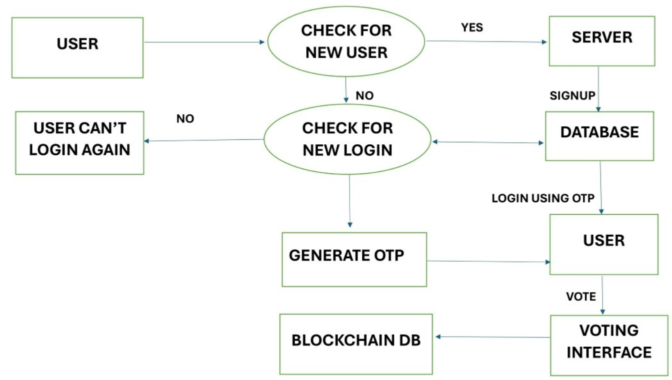

Fig. 1. System Design of Blockchain-Powered Electronic Voting Application

OTP verification. Since every block in the blockchain shares the same distributed ledger, all of the contents and information required by each block in the blockchain are kept in a blockchain database that is implicit in Ethereum. The system design is illustrated in Fig. 1. According to the architecture of the system, Blockchain and database are storage entities. When a user registers or logs in to the voting portal, their information is uploaded to the database if it isn't already there, and an OTP is generated and delivered to them. Once the OTP is correctly submitted, the user can vote for the candidate of their choosing. The blockchain contains the candidate's information and the total amount of votes they have earned.

Discussions about blockchain technology are taking center stage in the finance and technology industries. But blockchain has much more potential than just supporting cryptocurrencies like Bitcoin, which is its most well-known use. Online voting systems are among the fields where blockchain technology could have a big influence. The election commission and the voter are its two primary constituents. There are stages in the ER diagram: the registration phase, the login phase, and the voting phase as shown in Fig. 2.

Online voting, often known as e-voting, has long been discussed and holds the potential to improve accessibility and efficiency in the electoral process. However, there have also been several difficulties with trust, privacy, and security. Herein lies the use of blockchain technology. The decentralized and secure ledger technology known as blockchain provides several benefits that have the potential to completely transform online voting:

1. Transparency and Immutability: Transactions are recorded across several computers in a distributed ledger or blockchain. Votes are permanent and unchangeable once they are registered on the blockchain. This transparency and immutability improve the electoral process's integrity by guaranteeing that a vote cannot be changed or manipulated once it has been cast.

2. Security: Blockchain protects transactions with cutting-edge cryptography methods. In the context of voting, this means that ballots are safe and encrypted, lowering the pos-

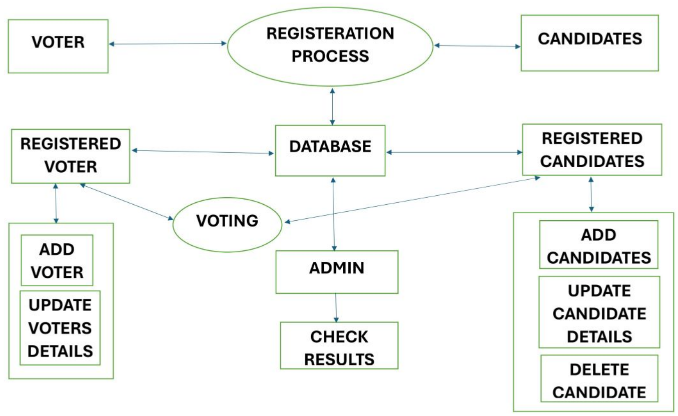

Fig. 2. ER Diagram of Blockchain-Powered Electronic Voting Application

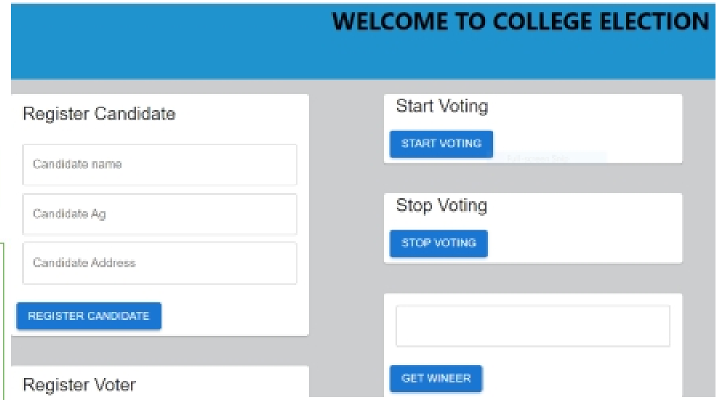

Fig. 3. Frontend of Blockchain-Powered Electronic Voting Application

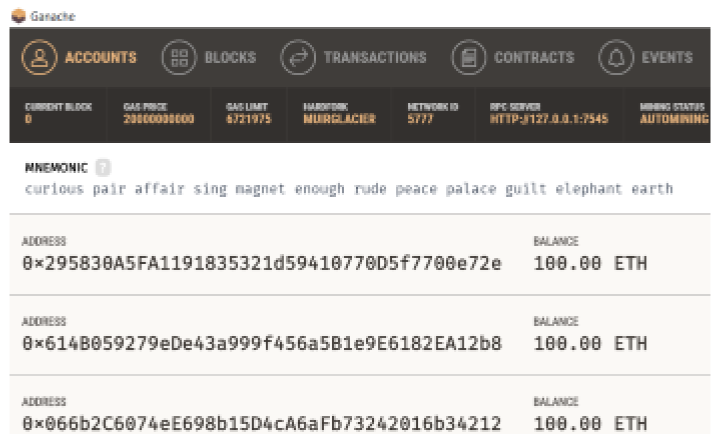

Fig. 4. Ganache: personal blockchain to deploy and test smart contracts

sibility of fraud or hacking. Every voter has a private key, which ensures that the results are confidential and that only those with permission can view them.

3. Decentralization: Conventional voting methods sometimes depend on centralized authorities for the management and supervision of elections. Blockchain, on the other hand, does not require a single central authority because it runs on a decentralized network of computers. This lowers the possibility of voting process manipulation or intervention.

4. Accessibility: Voting online with blockchain technology can facilitate voting for people. Using a computer or mobile device, voters can cast their ballots without leaving the comforts of their homes and without having to go to physical polling places. Voter turnout may rise as a result, especially among those who live in rural regions or have transportation challenges.

5. Verification: Voters can use blockchain technology to instantly validate their ballots, promoting trust and transparency. Voters can verify the validity of their ballots using this cutting-edge technology without jeopardizing their anonymity. The electoral process is made more transparent by the use of blockchain, which securely records each vote and allows the voter to verify it. This method preserves privacy while guaranteeing transparency, enhancing trust in the precision and dependability of the voting process.

IV. Analysis and Discussion

This section provides an analysis of the online voting system using blockchain applications. In this application, there are many functions present and each function has its role. There are some important functions and these are: Register Candidate, Register Voter, Start Voting, Stop Voting, Get Winner, Get All Candidates.

The function Register Candidate is used to register the candidates who want to stand in the election. The register Candidate function takes the three inputs and these are Candidate name, Candidate age, Candidate address. The function Register Voter is used to register the candidates who want to vote in the election, the voter can register only if the voter has a minimum age of 18. The Register Voter function takes the Voter address as input. The Start Voting function is used to start the elections. The stop voting function is used to stop the elections. If the time of the election gets over then voting can be stopped by using the Stop Voting function. Front-end of the application is shown in Fig. 3. Ganache as shown in Fig. 4 is also used in creating this Online Voting System Using a blockchain application. Ganache is a personal blockchain, that is used for the development of distributed applications for Ethereum. Ganache can be used across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment. Metamask is also used in creating online voting systems using blockchain applications. As a non-custodial wallet, MetaMask as shown in Fig. 5 gives users complete control over their private keys at all times. Connecting users securely to various blockchain-based applications and enabling them to explore the decentralized Web 3.0 is what makes it special.

This section also provides a thorough analysis of the average execution time, average latency, and average throughput for two well-known blockchain platforms: Ethereum and Hyperledger Fabric. The findings displayed in Figs. 6 and 7

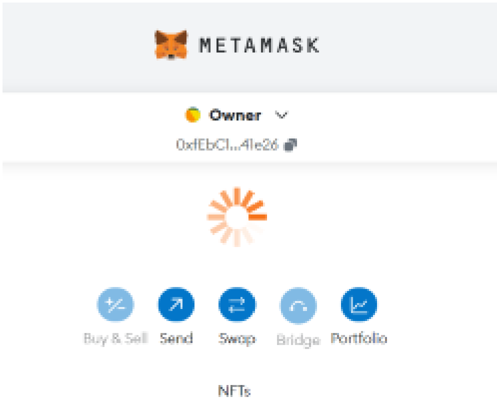

Fig. 5. Metamask tool for processing transactions and interfacing with decentralized apps on the Ethereum blockchain

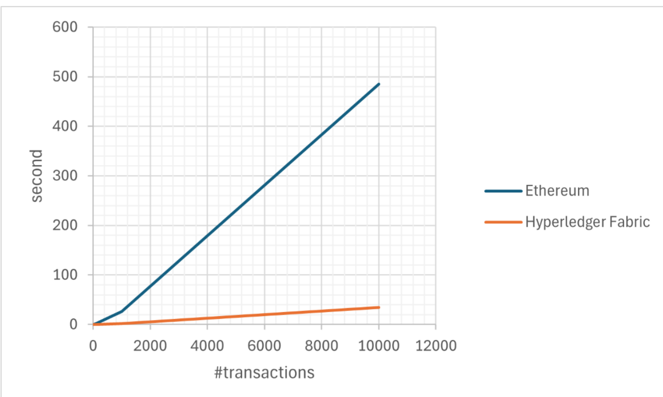

Fig. 6. Average delay of Ethereum and Hyperledger with a Varied amount of transactions of TransferMoney Function

offer insightful information on the relative advantages and disadvantages of these systems in various contexts.

Average Execution Time: The assessment starts by examining the variations in execution times for various quantities of transactions across various platforms and functionalities. Overall, it's evident that Hyperledger Fabric performs better than Ethereum in every situation. It is projected that both systems' execution times will lengthen as the number of transactions in the dataset rises.

A noteworthy feature is the difference in execution times between Ethereum and Hyperledger, where Hyperledger often shows faster execution times. The more transactions there are, the greater the gap gets. Three different functions are compared in terms of execution time: CreateAccount, IssueMoney, and TransferMoney. Since CreateAccount is a built-in feature for both systems, its execution times are comparatively shorter. Nonetheless, the unique features created for this fictitious application—IssueMoney and TransferMoney—highlight notable variations in functionality.

Average Latency: The average latency experienced by TransferMoney transactions in five sets of experiments for

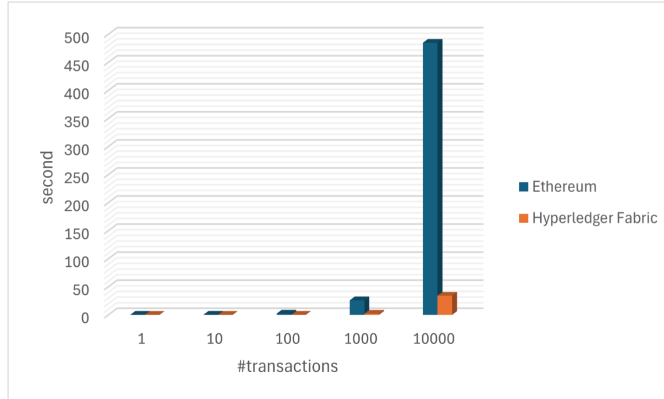

Fig. 7. Comparison of the average latency of Ethereum versus Hyperledger

each platform is plotted in a log-log fashion in Fig. 6, which represents the analysis of average latency. Hyperledger Fabric has an average latency of 0.09 seconds even when there is only one transaction in the dataset, but Ethereum has an average latency of 0.21 seconds. The context for comprehending the scalability and responsiveness of both platforms is established by this preliminary comparison. Ethereum's latency regularly turns out to be rough twice that of Hyperledger at smaller transaction numbers as the dataset's transaction count increases. Nevertheless, Ethereum's latency is noticeably worse than Hyperledger's as transaction volume rises. This trend is further highlighted in Fig. 7, which compares the average delay across five sets of tests for each platform. The average latency for both systems increases noticeably as the number of transactions in the dataset increases, according to the log-log plot. This emphasizes the difficulties Ethereum and Hyperledger Fabric have in keeping latency low despite growing workloads. Hyperledger Fabric offers lower average latency compared to Ethereum, making it a more scalable and responsive solution, especially in high transaction volumes.

Implications for Throughput: Although throughput is not specifically mentioned in the language that is provided, it can be assumed based on the execution time and latency data. The number of transactions executed in a given amount of time, or throughput, is a crucial indicator of a blockchain system's overall performance efficiency. The constant superiority of Hyperledger Fabric over Ethereum in terms of execution times and latency directly translates into increased throughput. Hyperledger Fabric is a more performant option for applications where speed and responsiveness are critical due to its efficiency in transaction processing.

Our approach does away with the requirement for extra tools like testrpc and ganache, which are sometimes needed for older approaches to generate test ethers. Instead choose a simpler strategy in which mine the ethers to produce them. This guarantees a self-sustaining method for resource development within system in addition to simplifying the process.

Scalability is a crucial factor in managing an increasing volume of users and transactions, and it is accomplished by combining the blockchain file system with MongoDB.

Together, these approaches enable effective block-specific data storage. The system is well-suited to handle a rising amount of data without sacrificing performance by making use of these scalable methods.

The suggested voting method is essentially an easy-to-use, safe, and effective fix. It provides simplicity and user-friendliness, works with a private blockchain for increased security, and does away with the need for additional tools. One of the main goals is scalability, which is accomplished by combining a blockchain file system with MongoDB. Improve security and streamline the system's logic by limiting voting access to legitimate users with confirmed national IDs.

V. Conclusion and Future Perspective

The study on the application of blockchain technology to online voting systems concludes this research paper with a picture of a world full of opportunities to improve and revolutionize democratic procedures. Examining the problems included in conventional voting methods and looking for novel approaches by using blockchain, we discover a route that offers improved safety, openness, and usability in the electoral sphere. This conclusion highlights the significant changes that could occur to the democratic fabric of civilizations worldwide and summarizes the complex ramifications of implementing blockchain-based online voting systems. The most significant benefit of using an online voting system based on blockchain technology is the unparalleled security it provides to the electoral process. Blockchain offers a strong answer to these problems thanks to its decentralized architecture and cryptographic concepts. A vote is virtually unchangeable once it is recorded thanks to the blockchain ledger's immutability. This not only reinforces the voting process's integrity but also gives voters more confidence, which promotes faith in the democratic system. The transparency that is built into blockchain technology strengthens the security component even further.

We need to discuss future research directions as we wrap up this study on the application of blockchain technology to online voting systems. Although the research to date has illuminated the revolutionary effect of blockchain technology on the safety, openness, and usability of the voting process, there are still many areas that are ready for more study and advancement. Researchers, decision-makers, and practitioners can further investigate and improve the incorporation of blockchain technology into online voting systems by following the roadmap for future work presented here. Because democratic processes and technology are dynamic, it is necessary to make continuous efforts to address new difficulties and take advantage of chances for progress. Blockchain can completely transform how societies conduct the basic act of casting ballots, so reshaping the face of democratic governance in the future.

References

[1] Jafar, U., Aziz, M.J.A. and Shukur, Z., 2021. Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17), p.5874.

[2] S. Jain, U. Rastogi, N. Bansal and G. Kaur, "Blockchain Based Cryptocurrency for IOT," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 744-749.

[3] Taş, R. and Tanrıöver, Ö.Ö., 2020. A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), p.1328.

[4] Hoffman, M.R., Ibáñez, L.D. and Simperl, E., 2020. Toward a formal scholarly understanding of blockchain-mediated decentralization: A systematic review and a framework. Frontiers in Blockchain, 3, p.35.

[5] Righetti, R., 2023. Blockchain in the public sector: an international census and a case study of public administration collaboration.

[6] Alves, J. and Pinto, A., 2019. On the use of the blockchain technology in electronic voting systems. In Ambient Intelligence–Software and Applications–, 9th International Symposium on Ambient Intelligence (pp. 323-330).

[7] Scheme, M.A.E., 2003, May. A Secure and Optimally Efficient. In Advances in Cryptology–EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings (Vol. 1233, p. 103). Springer.

[8] 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.

[9] Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," 2011 International Conference on Intelligence Science and Information Engineering, Wuhan, China, 2011, pp. 426-429.

[10] Yi, H. Securing e-voting based on blockchain in P2P network. EURASIP J. Wirel. Commun. Netw. 2019, 2019, 137.

[11] R. Patel, A. Sethia and S. Patil, "Blockchain – Future of Decentralized Systems," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 2018, pp. 369-374.

[12] Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. Comput. Sci. Rev. 2020, 36, 100235.

[13] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) 46, May 2008.

[14] Kiayias, A. and Yung, M., 2002, February. Self-tallying elections and perfect ballot secrecy. In International Workshop on Public Key Cryptography (pp. 141-158).

[15] Hao, F., Ryan, P. Y. A., and Zielinski, P. (2010) Anonymous voting by two-round public discussion, IET Information Security, vol. 4, no. 2, pp. 62-67, June 2010.

[16] Multichain (2017) Open platform for blockchain applications. Available at: www.multichain.com last accessed: December 2017.

[17] McCorry, P., Shahandashti, S. F. and Hao. F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[18] Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H., 2018, November. Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.

[19] Hanifatunnisa, R. and Rahardjo, B., 2017, October. Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.

[20] Ahmed Ben Ayed. A CONCEPTUAL SECURE BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM International Journal of Network Security and its Applications (IJNSA) Vol.9, No.3, May 2017.

[21] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. International journal of Innovative research in Computer and Communication Engineering, 4(4), 2016.

[22] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7:24477–24488, 2019

[23] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of india's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and Communications Security, pages 1–14, 2010.

[24] Shahzad B., Crowcroft J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access. 2019;7:24477–24488.

[25] Gao S., Zheng D., Guo R., Jing C., Hu C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. IEEE Access. 2019;7:115304–115316.