

Implementation of Secured Online Voting System using Blockchain Technology

Dharani J¹, Rajkumar T², Rathiya R³, Backiyalakshmi G⁴, Debila G⁵ and Indhumathi C⁶

¹⁻³Assistant Professor/IT, Dr. NGP Institute of Technology, (An Autonomous Institution), Tamilnadu, India

Email: dharani.j@drngpit.ac.in, rajkumar.t@drngpit.ac.in, rathiya.r@drngpit.ac.in

⁴⁻⁶Department of Information Technology, Dr.NGP Institute of Technology, (An Autonomous Institution), Tamilnadu, India

Email: gbakiya2@gmail.com, debilag33@gmail.com, indhu7200@gmail.com

Abstract—The primary aim of this paper is to propose a feasible solution to the obstacles encountered in digital voting by leveraging blockchain technology. Presently, the voting systems such as Electronic Voting Machines (EVMs) and paper ballots are not without flaws. These issues range from limited transparency, low voter turnout, vote manipulation, and mistrust in the election commission. Thus, there is a pressing need for a secure and trustworthy digital voting system that can protect against potential cyber-attacks or hacking. Blockchain technology presents a plausible solution to these concerns by offering numerous benefits, including decentralization, security, transparency, immutability, and anonymity. Blockchain technology facilitates the transfer of digital assets through a decentralized network by utilizing a widely used ledger. Blocks make up the ledger, a crucial component of blockchain technology that records all transactions. Our article suggests an electronic voting mechanism based on smart contracts for the Ethereum network. These contracts are a recent innovation that can provide a more reliable, transparent, and secure e-voting system. Using wallets and the Solidity programming language, we have tested and implemented this system. We can ensure the security and dependability of the voting process by leveraging blockchain technology and smart contracts for the electronic voting system. Any democratic system must retain this to remain legitimate.

Index Terms— Decentralized applications, Blockchain, Web 3.0, Solidity, Hardhat, System, Peer-to-peer Network, Ethereum Blockchain, Ethereum Virtual Machine, Smart Contract.

I. INTRODUCTION

Electronic voting machines have been used to increase vote accuracy and efficiency, but questions about their security and transparency have been raised. By building a safe and transparent voting platform, blockchain technology offers a solution.

A blockchain-based electronic voting system would take advantage of blockchain's decentralized nature to guarantee the accuracy of the voting process. Cryptographic techniques would provide anonymity and confidentiality, and each vote would be recorded as a tamper-proof transaction on the blockchain. This would result in a more secure, transparent, accurate, and cost-effective voting process compared to traditional electronic voting systems.

Adopting a blockchain-based voting system would bring numerous benefits, including increased security, transparency, and accuracy. It would also provide a more efficient and cost-effective solution compared to

traditional electronic voting systems. However, proper design and implementation are crucial to prevent vulnerabilities and attacks on the system.

The limitations and concerns associated with traditional electronic voting systems have created a need for a more secure platform for conducting elections. The challenges include issues of security, transparency, accuracy, and public trust in the electoral process. Given the growing concerns over the integrity of elections, developing a secure and transparent platform for voting has become crucial.

By providing a decentralized, secure, and tamper-proof platform for holding elections, blockchain technology offers an effective remedy to these restrictions. Implementing a secure electronic voting system powered by blockchain has the potential to boost voter confidence in the electoral process, increase voting efficiency and accuracy, and create a more transparent and secure election environment.

Blockchain-based secure electronic voting systems provide a solution to the problems with conventional electronic voting systems. To guarantee the accuracy of the voting process, blockchain technology makes use of decentralization. Each vote is confirmed by several network nodes and entered as a transaction on the blockchain. Voting integrity and confidentiality are ensured via cryptographic algorithms, such as digital signatures.

Once a vote is recorded on the blockchain, it is permanent and unalterable, making it almost impossible to tamper with the results. During the election, voters can securely cast their votes through a user interface, and their votes are added to the blockchain as encrypted transactions. The blockchain network then verifies the validity of the votes and adds them to the permanent ledger of election results.

In conclusion, the blockchain-based secure electronic voting system offers an open, effective, and impenetrable platform for holding elections. This method has the potential to change the way elections are conducted by leveraging the benefits of blockchain technology and increasing public confidence in the electoral process.

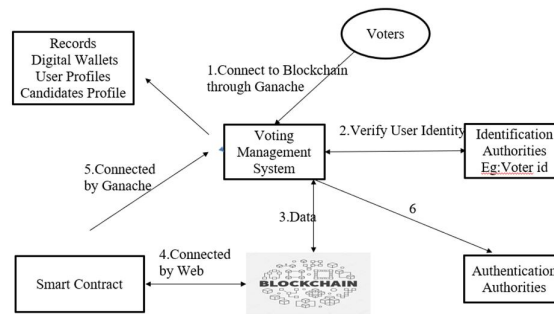
Blockchain technology can be used to create safe electronic voting systems, but how well they are implemented and how secure they are overall will affect how secure they are. Blockchain provides a high level of security against fraud and tampering, making it an advantageous option for electronic voting. It is challenging for attackers to compromise the system because of the decentralized structure of blockchain, which eliminates the potential of a single point of failure. Furthermore, cryptographic algorithms, including digital signatures and encryption, are used to ensure that each vote is authentic and confidential, making it challenging for anyone to manipulate the results.

II. LITERATURE SURVEY

- [1] Geethanjali Rathee, Razi Iqbal, Omer Waqar, Ali Kashif Bashir (2021) Utilizing Blockchain technology, an e-voting system can be established through IoT devices that offer both security and transparency. This technology can detect and address potential threats posed by unauthorized access at different levels.
- [2] Ehab Zaghloul, Tongtong Li, Jian Ren (2021) The suggested approach ensures protection against potential security risks while preserving voter anonymity. The performance evaluation and simulation results on smartphones validate the feasibility of the proposed method for conducting large-scale elections.
- [3] Suryaa Pranav Meduri, Saketh Kamatham, Sneha Subramaniam (2021) Initially, the voter undergoes authentication through their voter ID particulars and SMS e-verification. To achieve quicker and more precise outcomes, the system employs .Net and JavaScript for most client-side computations.
- [4] Huilin Li, Yinnan Li, Yong Yu, Baocang Wang, Kefei Chen (2021) The e-voting system proposed incorporates multi-choice voting and self-tallying capabilities. Its key objectives are to guarantee anonymity, time-constrained privacy, linkability, and complete traceability.
- [5] Somnath Panja, Samiran Bag, Feng Hao, and Bimal Roy (2020) The proposed Borda count-based ranked-choice electronic voting system uses a decentralized, self-tallying protocol. This protocol does not require a trusted setup or a central authority to compute the tally, in contrast to conventional techniques.
- [6] Ramya Govindaraj, Kumaresan P, K. Sree Harshita (2020) The article proposes an online voting system that allows voters to participate remotely. The system's framework is built using SQL server, and Microsoft Azure cloud, and programmed with C#. One crucial component of the administrator portal is to authenticate voters' identities before they are registered into the system.
- [7] Shlyao Gao, Dong Zheng, Rui Guo, Chunming Jing, Chencheng Hu (2019) Blockchain technology is used in the proposed e-voting protocol to guarantee voting process transparency. This approach is ideal for smaller-scale elections and offers several benefits in terms of security and efficiency.

[8] Dharshan Vishwasrao Medhane, Arun Kumar Sangaiah(2018) The suggested algorithm employs computational intelligence to protect content in e-Governance by utilizing a rule-based methodology derived from computational intelligence, as well as the current position information of users.

III. METHODOLOGY



After the voter casts their ballot, the approach is applied. The voter UI is used to register the vote. The transaction ID and timestamp are noted, and after data hashing and induction in a node, it is added to the blockchain. Without using a third party, the findings can be retrieved directly. Blockchain offers a completely cryptographically secure, decentralized system. Once data has been submitted, it cannot be changed without a correct sequence of events.

Blockchain:

Blockchain is a decentralized ledger system that makes transactions secure, open, and impervious to manipulation. It is simply a database shared by a network of computers that is updated and maintained by consensus. A chain of blocks is formed when a blockchain's blocks are connected by a unique identifier (hash) that links each block to the one before it.

Because of this chain, it is impossible to alter any data on the blockchain without also altering all subsequent blocks' hashes, rendering the blockchain impenetrable.

As the foundational technology behind the virtual currency Bitcoin, blockchain technology was first created. Voting systems, banking, and supply chain management are just a few of the sectors where it is now used.

Blockchain's decentralization eliminates the need for intermediaries like banks or government institutions to process transactions, resulting in faster and more efficient transactions, increased transparency, and enhanced security. Furthermore, the immutability of blockchain ensures that transactions cannot be altered, promoting data integrity and reducing the risk of tampering or fraud.

Elections could be held in a way that is transparent, safe, and impenetrable thanks to blockchain technology. In a decentralized system, voters can directly cast their ballots and be confident that their votes will be counted accurately and securely.

The voter's unique identity is included in each vote's blockchain transaction record. Voter privacy may be ensured using cryptographic methods such as zero-knowledge proofs. The immutability of blockchain technology guarantees that once a vote is registered, it cannot be modified, ensuring the validity of the results of the election. The decentralized nature of blockchain makes it difficult for malevolent actors to alter the outcomes because doing so would require them to have control over the majority of the network's nodes.

One of the challenges of implementing a blockchain-based voting system is ensuring that the system is accessible to all eligible voters, including those without access to the internet or those who are technologically unsavvy.

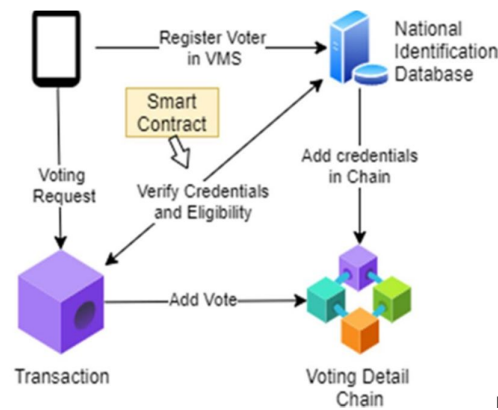
Electronic voting systems face challenges that can be addressed through various solutions, such as providing paper ballots as backups or deploying voting kiosks in public places. However, a blockchain-based voting system shows potential as a more secure, efficient, and transparent approach to conducting elections, although it requires careful consideration and addressing of its challenges.

Blockchain technology uses cryptography to create a decentralized, distributed ledger that offers secure data storage and transaction recording. Transactions are validated and stored by nodes in the network, and once they are added to a block, they cannot be modified, ensuring the immutability of the data.

Due to blockchain's adaptability, it has found use in several sectors, including voting systems, supply chain management, and banking. For instance, it facilitates secure cryptocurrency transactions and payment processing in finance, helps track goods and verify their authenticity in supply chain management, and enables secure and transparent voting processes in voting systems. Moreover, it allows for the creation of smart contracts, which are agreements whose terms are directly coded into the blockchain, bypassing intermediaries, reducing costs, and enhancing efficiency.

Smart contract:

A smart contract is a piece of software made up of both code and data that runs on the Ethereum virtual engine. With the option to partially or fully implement contractual clauses, these contracts are made to be self-executing and self-enforcing. Three steps make up the process of using a smart contract. The contract must first be made, generally using Solidity, a language that enables user collaboration on the blockchain. The smart contract is then added to the network and given a unique address on the blockchain so that all nodes can access it through a peer-to-peer network. Finally, the contract is automatically executed when certain pre-programmed conditions are met. All transactions resulting from the execution of the contract are recorded on the blockchain and cannot be reversed, making them traceable and transparent.



IV. SYSTEM DESIGN

Proposed system

The Ethereum blockchain's consensus mechanism is used to enforce the proposed protocol's execution as we implement it using the smart contract. To ensure that the voting process is followed, we suggest implementing our system as a smart contract on Ethereum. We are utilizing Ethereum since it can store and run smart contract-written programs.

Voter ID verification

A list of eligible voters is often compared with a voter's government-issued identification, such as a passport or driver's license, to confirm their identity. This method provides a moderate level of security, but it could potentially prevent eligible voters who do not possess government-issued identification from voting.

Two-factor authentication

Two-factor authentication involves using a combination of methods, such as biometric authentication and a password or PIN, to verify the identity of the voter. This technique offers a high level of security because it needs several different types of identification to access the voting system.

System features

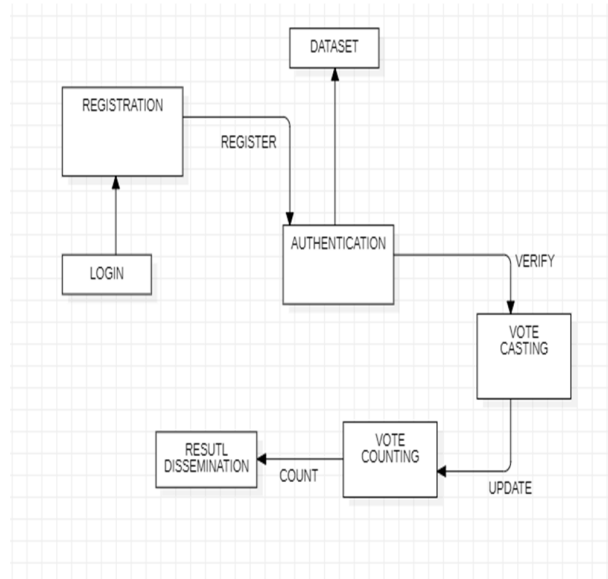
The problem analysis stage of software development serves as the foundation for the design and development phases. The issue is examined to gather enough information to build a new system. To simplify understanding and facilitate finding answers, big problems are broken into smaller ones. The tasks for this project are all grouped into several categories.

Advantages

The online voting system using BCT advantages are,

- Improve the security for voter's privacy.

- Immutable and decentralized system.
- No third party members.
- Less expensive



System module

- Voter Registration
- Voter Authentication
- Vote Casting
- Vote Counting
- Result Dissemination

Voter Registration

Voter registration is an essential step in the election process since it guarantees that only eligible voters can cast a ballot. In a secure electronic voting system using blockchain technology, voter registration typically involves the following steps:

Eligibility verification: The first step in voter registration is to verify that each potential voter is eligible to participate in the election. This typically involves checking that the voter meets the legal requirements for eligibility, such as being of a certain age and having the right to vote in the jurisdiction where the election is taking place.

Identity verification: Once the eligibility of a potential voter has been established, their identity must be verified. This typically involves using a secure form of identification, such as a government-issued ID, a passport, or a biometric identifier.

Voter registration: After the eligibility and identity of a potential voter have been verified, they can be registered in the system. This typically involves creating a unique digital identity for the voter that is stored on the blockchain, along with their personal information and voting history.

Voter authentication: Once a voter has been registered, they can use their digital identity to authenticate themselves when they go to vote. This typically involves using a secure form of authentication, such as a digital signature or biometric scan, to verify the voter's identity and prevent fraud.

Voter education: To ensure that all registered voters understand how to cast their vote securely and accurately, it is important to provide voter education and training. This typically involves providing information about the voting process, how to use the electronic voting system, and what to do if there are any issues or problems with the vote.

Voter Authentication

A technique for using blockchain technology to confirm the identification of voters in an election is called voter authentication by blockchain. A blockchain-based digital identity management system is used in this method to

verify a voter's identification. An individual's name, address, and government-issued ID number would be securely maintained and managed by this system.

The voter would have to present their digital identification during the voting process, and that identity would be checked against the data kept on the blockchain. As a result, each voter's vote would only be counted once, and their identification would be accurately documented. Also, keeping vote data in a safe and impenetrable manner using blockchain technology will make it more difficult for fraudsters to rig the results.

Vote Casting

Blockchain-based electronic voting refers to the process of electronically casting a vote and having that vote recorded on a blockchain ledger. Voters would cast their ballots under this system using electronic devices like computers or mobile phones. A safe and impenetrable record of the vote would then be created by encrypting it and recording it on a blockchain ledger.

For electronic voting systems, using blockchain technology has several advantages. Making a permanent and irrevocable record of every vote first assures the security and integrity of the voting process. This makes it difficult for fraudsters to manipulate the results and undermines confidence in the election. Secondly, it allows for increased transparency, as the blockchain ledger can be made publicly accessible, allowing anyone to verify the accuracy of the vote count.

While using blockchain technology in electronic voting systems has the potential to increase the security and transparency of elections, this technology is still in its infancy, and there are just a few elections where it has been used. Further research and testing are needed to determine the feasibility and security of this approach. Additionally, there are still many technical and logistical challenges to overcome, such as ensuring the security and privacy of voters' personal information, and ensuring that electronic voting systems are accessible and user-friendly for all eligible voters.

Vote Counting

In electronic voting systems, vote counting is the process of totaling and computing the results of an election that was held with the use of electronic voting machines. It is an important procedure that guarantees the accuracy and integrity of the election results.

Electronic voting machines gather and store the votes in a central database, and then specialized software is used to automatically process and tally the votes. This method is generally faster and more efficient than traditional paper-based systems, as it reduces the possibility of human error.

However, electronic voting systems also present potential risks, such as the chance of software failure or hacking. To address these concerns, multiple layers of security are incorporated into electronic voting systems, and they undergo strict testing and certification procedures before being implemented in elections. Some systems may also provide a physical record of the votes, allowing for a manual recount if necessary.

Result Dissemination

In electronic voting systems, the results are typically disseminated through a central database or website. The database or website contains the final vote totals for each candidate or issue, and the results are updated in real-time as the votes are processed and tabulated. This allows for quick and efficient dissemination of the results, making it easier for the public to access and understand the outcome of the election.

Additionally, certain electronic voting systems could include thorough results information, such as the total number of votes cast in each precinct or a breakdown of votes by demographic category. By using this data, the electoral process can be made more transparent and accountable.

Before being deployed in an election, electronic voting systems are normally subjected to stringent testing and certification procedures to verify the accuracy and integrity of the results. A manual recount may be possible if necessary because some systems may also give a paper trace of the votes cast. To further strengthen transparency and legitimacy, the election results may also be audited by unaffiliated third parties.

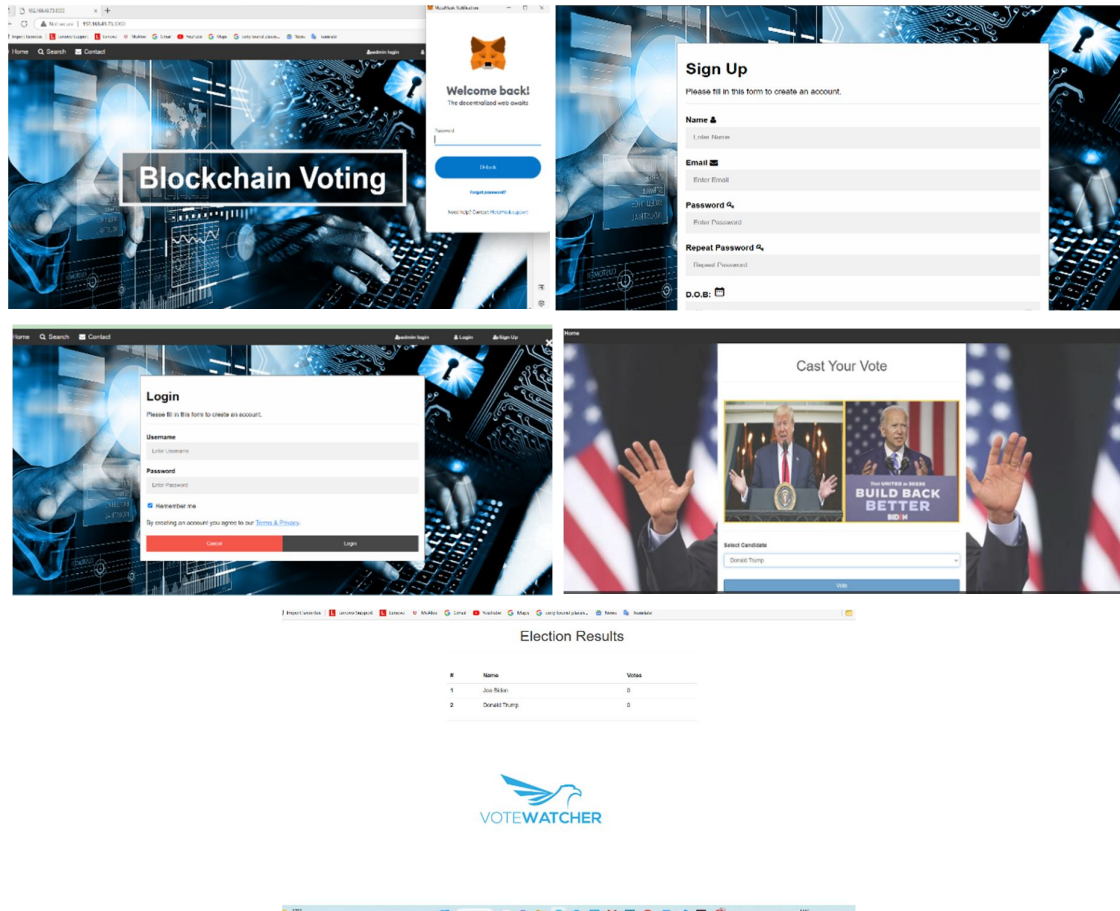
V. RESULT AND DISCUSSION

To ensure a fair and democratic election, it is essential to assess electronic voting systems based on their security, accuracy, accessibility, transparency, and user experience. Security is paramount to prevent any tampering or malicious activities that could compromise the election results. The accuracy of the system is also critical to ensure that the election results reflect the voters' will.

To ensure that all eligible voters, including those with impairments, can cast their ballots, accessibility is crucial. The voting system must be user-friendly and efficient to use, providing a positive user experience for voters.

Additionally, transparency is crucial in building trust in the election results by allowing auditing and verification of the election results.

Electronic voting technologies have the potential to enhance the voting process, boost voter engagement, and decrease mistakes. However, it is essential to carefully evaluate these systems to ensure that they meet the needs and expectations of voters and election officials. By considering the factors of security, accuracy, accessibility, transparency, and user experience, we can ensure that electronic voting systems are reliable, trustworthy, and democratic.



VI. CONCLUSION

The model for an internet voting system for India is described in this essay. Compared to the current voting system, the proposed system is both significantly safer and more effective. Vote tampering and a delay in results are easily avoidable. Our suggested model is based on a singular AADHAAR identity. It results in simpler voter and candidate verification. The goal of the proposed framework was to provide a safe online voting system that voters could use to cast their ballots without worrying about unwanted access. The suggested system's server components are configured with a distribution of power that prevents vote rigging. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system.

REFERENCES

- [1] Geethanjali Rathee, Razi Iqbal, Omer Waqar, Ali Kashif Bashir(2021), "On the Design and Implementation of a Blockchain-Enabled E-Voting Application Within IoT-Oriented Smart Cities," date of publication February 23, 2021, DOI 10.1109/ACCESS.2021.3061411.
- [2] Ehab Zaghloul, Tongtong Li, Jian Ren(2021), "d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting," IEEE Internet Of Things Journal, VOL. 8, NO. 22, November 15, 2021.

- [3] Suryaa Pranav Meduri, Saketh Kamatham, Sneha Subramaniam(2021),“ A Secure Network Monitoring Balloting System,” in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.
- [4] Huilin Li, Yannan Li, Yong Yu, Baocang Wang, Kefei Chen, “A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era,” IEEE transactions on network science and engineering, VOL. 8, NO. 2, APRIL-JUNE 2021.
- [5] Somnath Panja, Samiran Bag, Feng Hao, and Bimal Roy, “A Smart Contract System for Decentralized Borda Count Voting,” IEEE transactions on engineering management, VOL. 67, NO. 4, NOVEMBER 2020.
- [6] Ramya Govindaraj, Kumaresan P, K.Sree Harshitha, “Online Voting System using Cloud,” International Conference on Emerging Trends in Information Technology and Engineering,2020.
- [7] Shlyao Gao, Dong Zheng, Rui Guo, Chunming Jing and Chencheng Hu, “An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function”, date of publication August 16, 2019.DOI 10.1109/ACCESS.2019.2935895.
- [8] Darshan Vishwasrao Medhane and Arun Kumar Sangaiah, “PCCA: Position Confidentiality Conserving Algorithm for Content-Protection in e-Governance Services and Applications,” IEEE transaction on emerging topics in computational intelligence, VOL. 2, NO. 3, June 2018
- [9] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. "Blockchain-based e-voting system." In *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pp. 983-986. IEEE, 2018
- [10] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." *International Journal of Network Security & Its Applications* 9, no. 3 (2017): 01-09.
- [11] Garg, Kanika, Pavi Saraswat, Sachin Bisht, Sahil Kr Aggarwal, Sai Krishna Kothuri, and Sahil Gupta. "A comparative analysis on e-voting system using blockchain." In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1-4. IEEE, 2019.
- [12] Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." *Ieee Software* 35, no. 4 (2018): 95-99.
- [13] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain-based e-voting recording system design." In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1-6. IEEE, 2017.
- [14] Vivek, S. K., R. S. Yashank, Yashas Prashanth, N. Yashas, and M. Namratha. "E-voting systems using blockchain: An exploratory literature survey." In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 890-895. IEEE, 2020.
- [15] Singh, Ashish, and Kakali Chatterjee. "Secevs: Secure electronic voting system using blockchain technology." In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 863-867. IEEE, 2018.
- [16] Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." *Symmetry* 12, no. 8 (2020): 1328.
- [17] Jafar, Uzma, Mohd Juzaidin Ab Aziz, and Zarina Shukur. "Blockchain for the electronic voting system—review and open research challenges." *Sensors* 21, no. 17 (2021): 5874
- [18] Fusco, Francesco, Maria Iliana Lunesu, Filippo Eros Pani, and Andrea Pinna. "Crypto-voting, a Blockchain-based e-Voting System." In *KMIS*, pp. 221-225. 2018
- [19] Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." *International Journal of Electronic Government Research (IJEGR)* 14, no. 1 (2018): 53-62.
- [20] Shahzad, Basit, and Jon Crowcroft. "Trustworthy electronic voting using adjusted blockchain technology." *IEEE Access* 7 (2019): 24477-24488
- [21] Roh, Chang-Hyun, and Im-Yeong Lee. "A study on the electronic voting system using a private blockchain." *Journal of Information Processing Systems* 16, no. 2 (2020): 421-434.
- [22] Adiputra, Cosmas Krisna, Rikard Hjort, and Hiroyuki Sato. "A proposal of blockchain-based electronic voting system." In *2018 second world conference on smart trends in systems, security, and sustainability (WorldS4)*, pp. 22-27. IEEE, 2018.
- [23] Denis González, Camilo, Daniel Frias Mena, Alexi Massó Muñoz, Omar Rojas, and Guillermo Sosa-Gómez. "Electronic voting system using an enterprise blockchain." *Applied Sciences* 12, no. 2 (2022): 531