

# Revolutionizing Voting Security Using Blockchain

Kumar Sanjeev, Naveen Chander, Amrita Kumari, Saurabh Kumar  
Chandigarh University Punjab, India

*Abstract- In this democratic world, voting is an important event. And electronic voting is the current voting scheme through ballot or electronic voting. Using old voting systems has greater output and also less error, but still there is many challenges to achieve a transparent voting scheme. During a pandemic, citizens tend to panic due to a huge crowd where an offline voting system is lacking. Also, EVM(electronic voting machine) paper-based voting system schemes provide less transparency and huge risks of misleading the candidate's votes. The third-party role will be eliminated when we apply smart contract in the Ethereum network to bring perfect voting results.*

**Keywords:** *Electronic Voting, Blockchain, Efficiency, Smart contract, network.*

## I. INTRODUCTION

Democratic countries have the right to elect their representatives by voting for the right candidates during elections, as elections are important pillars for a free system that enables the clients to give their opinion in the form of vote. And, in this democracy, the protection of votes and transparency in the process should be reflected to the people. Moreover, the traditional voting system(paper ballot and EVM) demands a high investment of money and time, which does not surely promise transparency and security for the votes.

In the conventional voting system, voters have to register and wait for their voter card, which takes a huge amount of time. The voting process takes several days to be processed and also requires multiple employees and forces to ensure a smooth process. This old implementation has several issues that led to criticism because of interruptions such as unnatural climates as well as lengthy queues at polling stations.

Contrarily, the traditional E-voting system bridges shortcomings part such as integrity, reliability, isolation, and identification for example, accessing voters' information during the process might create the risk of potential hacking and unsanctioned manipulation. Hence, a high requirement to bring a transparent E-voting system that lets the voters vote

comfortably and efficiently, allowing election officials to declare the result openly.

Blockchain and Ethereum networks are rising technologies nowadays that hold tight encoding bases that enable software to hold great security solutions and integrity of the client. Recently, many researchers have started concentrating on Ethereum-based secure and transparent solutions in wide domains. Blockchain is a decentralised log operating on a peer-to-peer (P2P) network. It always uses encrypted symbols to communicate among different blocks. This technology provides potential security and challenges found in E-Voting systems.

In a recent survey, it is suggested that verification and registration most need updation in an E-voting system. This creates a crucial requirement to bring smart, secure contracts of blockchain to provide the required requirements. On this, we are moving to secure Electronic voting mechanisms we have designed the function used during voter registration and voting mechanisms. While applying cloud storage to manage the ballots.

This technology exhibits the potential to address more than one security issue and together ensure possible transparency in the electronic voting system. Several case studies conclude that verification and transparency are the areas required for updation, with this aim, we decided to move ahead to a reliable and secure E-voting System.

### A. RELEVANT CONTEMPORARY ISSUES:-

The traditional voting system has security, transparency and integrity issues. There is a huge risk of manipulation in voting. During the process of the personal data of voters, stores have a high risk of hijacking, which leads to threats to individuals. The traditional method requires a huge amount of manpower for successful voting mechanisms. Moreover, voters have to wait for so long hours in a queue for their turn to cast a vote, which decreases the number of hit ratio(number of voters who cast their votes/number of voter cards issued) of the voters. To overcome these issues, we designed an algorithm

using blockchain, which provides a secure, transparent and efficient way of voting process.

## B. IDENTIFICATION OF PROBLEM

Election plays an important role in democracy, and democracy can be achieved by voting securely. The ancient method of voting, like ballot voting, was creating problems as it required a lot of effort and money for the smooth execution of the process. Also, it is a very big problem for the management to execute the electoral process smoothly and make it successful. As citizens do not want to go to the voting station and engage in the rush process as this process includes the risk of life and arbitrariness of some big people.

## IDENTIFICATION OF TASK

In the offline voting system, there is a lack, so to overcome these issues, firstly, using blockchain, we will make the voting mechanisms secure by bringing a remote voting system. We make it comfortable, reliable, and accessible by introducing a remote voting system we can reduce the manpower and a huge investment. By implementing these tasks we will be able to make a centralised voting system for every state which makes the mechanism more transparent among citizens, politicians and officials.

## C. PROBLEM DESCRIPTION AND CONTRIBUTION

At the moment, several Electronic voting systems have been introduced, but they lack privacy and reliability and have different issues. The recent IOT and Blockchain-based solution introduced can be the solution to the discovered error in the voting mechanisms, but it is in the process. Blockchain will be a perfect solution for the Electronic voting process. Many implementations are tested and even used for some time however, every methodology is successful and good to be still in use. Also, there are many great electronic polling platforms available, but we still cannot declare the same for a voting system for the government.

## D. RELATED WORK

There are numerous electronic voting systems in use today, each with their own advantages and disadvantages. The most important problems to be found are those related to authentication, transparency, and security. One potential solution to these problems is the hybrid blockchain technology that has just been developed.

An Internet of Things (IoT), a transparent Web-voting system utilising blockchain, was introduced by Rathee et al.[6]. This approach is used in developed nations. This method works under the initial assumption that all parties are reliable. It recognises dangers posed by vote-rigging intrusions. A number of security metrics, including message modification, assaults and authentication latency, are used to compare the performances.

An end-to-end verifiable nearby Internet-operated survey of the Electronic voting system has been proposed by Pawlak et al. This method necessitates intricate calculations and offers little assurance regarding the voter's identity. As a result, only small-scale systems can use ABVS.

An election mechanism that is transparent and sustainable was introduced by Panja and Roy.[30]. In order to ascertain whether their vote was integrated and recorded throughout the voting and counting phases, respectively, the user enters the system using a unique code. As a result, voters have more faith in the system, which raises performance indicators like robustness and fairness.

Mccorry et al. proposed online electronic E-voting mechanisms that utilise contracts and a stretchable agreement mechanism to provide satisfactory outcomes. There are no polling places in this system's implementation. Nevertheless, achieving robustness, latency, and privacy significantly is challenging.

For authentication, Kumar et al. suggested a method that is a mixture of characteristics of the blind signature scheme. Furthermore, the data in the blockchain is securely transferred using the Diffie-Hellman assumptions. Distributed ledger technology (DLT) removes vote tampering and offers transparency. Every vote is encrypted using asymmetric cryptography, which is far quicker than the Adleman encryption techniques, allowing for voter authentication and repudiation. For key management and signature creation, ECC works well.

According to Yi, a modified E-voting system guards against ballot stuffing by guaranteeing the legitimacy of votes that have been cast.

The first blockchain-based transparent mechanisms which depends on direct recording which was introduced by Panja et al. The encryption technique, which reads encrypted communications without decoding them, using Paillier homomorphic method,

used in this electronic voting system. As a result, the system may validate voters by requesting their ID without disclosing their preferences, as demonstrated by 103 B. Jayakumari et al.

Faber et al. took advantage of cryptographic methods that were integrated with Ethereum in order to give voters security. It is demonstrated that a blockchain proof of concept maximises voter trust. A framework that uses a flexible consensus method to support an ascending blockchain was proposed by Frooq et al.. The voting system's chain security algorithm makes sure that the vote is successfully completed. Moreover, 51% of attack avoidance on the blockchain has been implemented. The evaluation of this framework demonstrates that a sizable population can use the system.

To prevent a ballot stuffing attempt, Ms Usha and Divya [39] suggested a unique solution that offered a solid and verifiable structure for user registration and for the casting of votes. To prevent the creation of an enemy, they upgraded their method, which was already implemented and used rectitude to enhance the system. Additionally, the author provided an explanation of the final total using trustworthy multi-party computation and NIZK proof.

When Jordan was absent due to an election process, Malkawi et al. devised a voting system. Malkawi presents a unique and safe electronic voting casting mechanism where voters cast their ballots on two different measures: one is for the group as a whole, and the other is for the individual. This mechanism uses a newly created algorithm to foster appropriate accuracy and results when building and voting voter ballots.

Goyal et al. [27] suggested organising the full election process on internet based platform by the Indian government by implementing the Ethereum network tool and also proposing an Electronic system. The suggested concept promoted using decentralised applications (dApps) to organise elections in India. It was inspired by this planned work to combine machine learning and data.

The IPFS Ethereum was a legacy tool used in Panja's [41] proposed framework. This framework suggested a fingerprint encryption method with an enhanced miss rate as a cryptographic method for secret ballot elections. This framework's limitation is less effective.

In order to determine the parameters for the implemented transaction flexibility setting up an

Electronic-voting system, in Niaz et al. [42] investigated the implemented voting system. The associated framework emphasises the significance of the network delay and block production rate as well as future research directions. Less is known about the anticipated work's limits. The writers made an effort to gain insight to the situation that takes the system to an attack.

In Killer et al. [43], they presented robust, flexible, and useful electronic voting system which fulfilled requirements of wide-scale elections while requiring minimal input by the electorate process.

The old voting system that works as the user's "black box" was build using a randomiser coupon which guarantee both invoice-less and imposition barrier. The adopted mechanism guaranteed an improvement in terms of efficiency and security.

A mixed agreement-based model that combines evidence of stake and evidence of credibility was proposed by Abuidris et al. [44]. In this investigation, the Amazon EC2 Ethereum tool in MATLAB was utilised. The execution of contracts pointed to establishing a robust, consistent computing system that would promise the integrity, safety and precision of the implemented process. The system is combined by the framework which guarantees the flexibility of the BC-based E-voting system. Arguments concerning how raids suggested that these should be carried out were conducted in order to assess the security effectiveness and guarantee receipt freeness and coercion resistance.

Suralkar et al. used the Ethereum tool, fingerprint authentication, ring signing, and BC technology to build a safe and protected E- based voting system. The system is more verifiable and safe since the suggested architecture does not require an excessive number of people at every level; however, this effort is less scalable.

In order to increase voter desirability and replace the traditional voting procedures used in the Near East and new world, Abo samra et al. developed a safe and examined crypto based Electronic voting mechanism. because of paper ballot mix-net foundation of the proposed electronic voting system, complicated protocols are needed to maintain shared mix keys. Furthermore, mix-nets would be complicated to build in a wide scale are prone to fudging. Testable and ballot safety are all provided by the suggested plan. Additionally, threat and firm evaluations were carried

out to demonstrate the systems' resistance to known threats.

Moura and Gomes investigated several requests that were turned down by BC. Although the purpose of this was to assess the application's potential with users, security and privacy risks have always existed.

Zeadally et al. investigated less concentrated BC application. The authors assessed BC's applicability from a quantitative standpoint as well as its impact on several applications that BC did not address. BC now possesses professional knowledge of the legal and technological aspects of digital services.

In order to prevent false vote selection by enhancing the security and dependability for the E-voting system, Ahn proposed the advance acquisition of blockchain-based E-voting method. A speculative two-step authentication approach for security reason in Ethereum based E-voting was implemented by González.

The most important problems found with the current electronic voting system include latency, response times, vote manipulation, authentication delays, and latency. Other problems include the voting system's lack of dependability, adaptability, security, and cost-effectiveness. To solve these problems, the suggested cloud-based online election system. Since only voters with valid voter registrations are able to cast ballots, it encourages dependability and transparency. Furthermore, votes that are manipulated may be substantially recorded and subsequently void. The implementation of blockchain technology, along with smart contracts and suitable consensus methods for encrypted ledgers and block recording, guarantees the safety of the electronic online election system. Furthermore, it seeks to reduce authentication latency or delay in comparison to traditional systems.

#### E. SUMMARY:

In the journey of our research about the mechanisms, the voting system process has numerous deficiencies. The issue of security, reliability, and manpower is a continuous barrier to the smooth functioning and a transparent voting system. We have discussed numerous methods to overcome issues like security, transparency, reliability, etc. We are going to implement an online Voting system with blockchain; Blockchain will remove the issue of security, while an online platform removes the error of reliability and manpower. We will deploy our algorithm to be more

accurate and secure than the already discovered method.

#### F. OBJECTIVES

Implementing a blockchain voting system has numerous key objectives which aim to enhance the issues (integrity, security and transparency) of voting mechanisms some of the primary objectives are as follows:

##### 1. Trust and Transparency:

- Objective: This ensures that all the processes recorded transparently and can be varied by any officials without compromising citizen's privacy.
- Benefits: This increases the trust between the voters and electoral process as anyone can verify the integrity of votes which reduce the overall disputes and frauds.

##### 2. Security:

- Objective: A secure voting system can stand out against hacking tempering fraudulent activities
- Benefits: We are using blockchain which uses cryptographic methods to protect data which ensures that votes cannot be manipulated.

##### 3. Accessibility:

- Objective: allow for more easily voting and enable people to vote remotely from different locations without an issue of process security.
- Benefits: Improves voting system and makes it more convenient for citizens.

##### 4. Cost reduction:

- Objective: Lower the cost required to run the physical infrastructure and other resources
- Benefits: Blockchain voting systems could reduce the need for physical polling stations and traditional resources.

#### G. CONCEPT GENERATION:

In this block, we are analysing the concept and implementation phase of our web page. The client can use our web application where they can register itself and also cast their votes in a secured and transparent environment. User have to register on the website with their unique id after whenever there is any election they can login and cast their vote for more security we use real time authentication by using blockchain we make the process more secure as blockchain and

Ethereum uses encoding method to hide the message of voters using different encoding method we maintain the database which includes name, gender, unique id after the election result voters can view the result on the web site also they can examine their vote which they had casted by using their unique address.

**H. DESIGN CONSTRAINTS:**

In this document, We are designing a secure web page where voters can vote and after declaration of result they can verify their vote using their public key. We use blockchain for security features and MySQL to manage database of voters we are using Ethereum network to provide a framework for blockchain creation and storage.

**Feature Selection:-**

We are enhancing the features and security of electronic voting system .

1. Security: We are using a real time authentication OTP verification and blockchain technology to make the process secure
2. Authentication: Every voters have to register with their unique id on their web page portal and whenever they wish to login they have to verify their identity using unique id and otp verification.
3. Database management: We are using SQL at the backend to manage the personal information of the voters uniquely.

**Feature Importance:-**

The feature we are including is an important element of an electronic voting system. We are enhancing the security as security Is the most important element to keep the integrity of the voting system for this encrypted algorithm used by blockchain is the best possible method . We also need to manage the database as there are huge risk of duplicate data or unauthorized login.

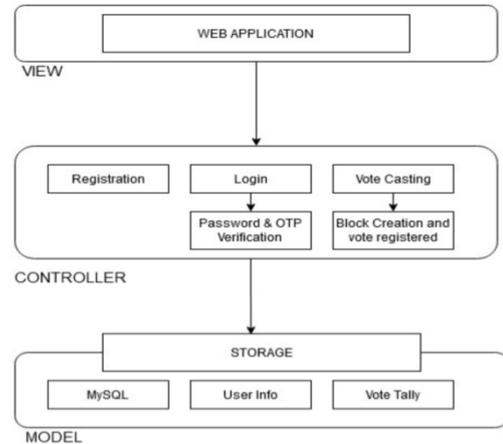
**II. RESULT ANALYSIS AND IMPLEMENTATION**

**A. IMPLEMENTATION**

The Web page is developed using an structural pattern of the MVC. It is a largely used structure . Our web page is divided into 3 elements: MVC(the model, the view, and the controller).

- **View:** This is the first layer in which the user interacts with the frontend using various elements. The views display the data from the model and allow users to interact.

- **Model:** It is the basic logic segment of any web page This is the data processing layer that handles data management and storing it.
- **Controller:** This is the middle layer of any application that performs the main functionality of the web page when the user interacts with the front-end controller responses, and all the functions that are required to run are performed through a controller.



**FIGURE-1: FLOWCHART OF WEB PAGE**

On our web page, to cast votes, users have to create their ID with a secret unique, and to cast votes, the user must have some Ethereum (a type of cryptocurrency that is required to perform any transaction), which is called a transaction fee. When users log in to our web page, they can see the database of the politician. In blockchain the reading data from blockchain is costless but writing need a minimal fee which means user can see the list of candidates free of cost but when they want to caste vote they have to pay a minimal transaction fee.

```

Database_API > .env
1  MYSQL_USER="root"
2  MYSQL_PASSWORD="@123"
3  MYSQL_HOST="localhost"
4  MYSQL_DB="voter_db"
5  SECRET_KEY="d2b861a623b1d0e89f7c91c313bce1db34fbce8356ca80
6  cf38b72e4c5a832ed5f0fa7136ef0ed5c32641308daa88c29c108d85835a
7  fc37e5385c8e2c4cacee6"
    
```

**FIGURE-2: LOGIN VERIFICATION CREDENTIALS IN MYSQL**

To create our login page, we use HTML in the form of the login form web page and create 1 label as voter id and another label for password and below both labels there is a button to submit.



FIGURE 3: LOGIN WEB PAGE

During login, our authorized user contract will run to verify whether the login is valid or invalid. After successful login user can see the list and caste votes.

```
// Authorization middleware
const authorizeUser = (req, res, next) => {
  const token = req.query.Authorization?.split('Bearer ')[1];

  if (!token) {
    return res.status(401).send('<h1 align="center"> Login to Continue </h1>');
  }

  try {
    // Verify and decode the token
    const decodedToken = jwt.verify(token, process.env.SECRET_KEY, { algorithms: ['HS256'] });

    req.user = decodedToken;
    next(); // Proceed to the next middleware
  } catch (error) {
    return res.status(401).json({ message: 'Invalid authorization token' });
  }
};
```

FIGURE-4: AUTHETICATION VERIFICATION CODE

In the database management system at the backend, we have to manage the data of the users who are login into the websites and who are casting the votes, and also their login credentials.

```
CREATE TABLE voters (
  voter_id VARCHAR(36) PRIMARY KEY NOT NULL,
  role ENUM('admin', 'user') NOT NULL,
  password VARCHAR(255) NOT NULL
);
```

FIGURE-5: TABLE CREATION UNDER VOTER\_DB DATABASE FOR MANAGING DATA OF USERS

We are creating a contract named voting, which takes an ID, name of candidates, name of the party, and vote count, and we map the count of candidates using a hash table and also keeping the address of Ethereum as bool because it can either be true or false.

```
contract Voting {
  struct Candidate {
    uint id;
    string name;
    string party;
    uint voteCount;
  }

  mapping (uint => Candidate) public candidates;
  mapping (address => bool) public voters;
```

FIGURE-6: CONTRACT CREATION FOR VOTING

We created a vote function that takes the unique candidate ID and checks whether the address of the candidate is true then the count of that particular candidate is increased by one, and in this way, the mechanisms work securely using blockchain.

```
function vote(uint candidateID) public {
  require((votingStart <= now) && (votingEnd > now));

  require(candidateID > 0 && candidateID <= countCandidates);

  //daha önce oy kullanmamış olmalı
  require(!voters[msg.sender]);

  voters[msg.sender] = true;

  candidates[candidateID].voteCount ++;
}
```

FIGURE-7: FUNCTION OF VOTE UNDER CONTRACT

B. RESULT:

A successful model is ready to launch in our electronic voting system. There is two options one for admin and another for client/voters.



FIGURE-8: ADD CANDIDATE AND DATE FOR VOTING WEB PAGE

- Admin: It might be an organisation or individual who organises the voting process for their candidates or for any third-party candidates. They have the access to change the candidate name or add more candidates or remove. They have real time access during the voting process. They can set a specified time period for the voting process.



FIGURE-9: VOTE PAGE

- Voters: They can sign in using a unique address, and voters can securely cast their vote for desired candidate by viewing the candidature list, they have at the bottom of their dashboard whether they have voted or not till that time they can also see the time period of voting and also they are able to see which candidate is leading.

### III. CONCLUSION AND FUTURE WORK

#### A. CONCLUSION:

This research, implemented an enhanced, secured Ethereum-based web page based E-voting system which includes a contract to provide security and enhancement in election by promising to hide the voter's personal information. Our crypto based technology provide more chances for the free nation in comparison to the old method. Nowadays, it is most important to keep updated according to technology and requirements.

Our model is more secure and transparent as there are so many elements that remove the barrier between voters and the voting system. Our mechanisms did not require a huge manpower and also a lot of money.

#### B. FUTURE WORK:

Electronic-based online voting system is always a difficult topic to resolve to the end conclusion, but many electronic voting systems performing stably, more different attempts might required to implement the secure and safety measures in the system, but it will be usable and scalable. On the other hand which we had designed using the contracts, Ethereum and the blockchain network have each security and privacy measures and also have voters verification of duplicate entry and transparency of counting. Also we can integrate a biometric authentication for more secure method

### REFERENCES

- [1] J. Huang, D. He, M.S. Obaidat, P. Vijayakumar, M. Luo, K.K.R. Choo, The application of the blockchain technology in voting systems: a review, *ACM Comput. Surv.(CSUR)* 54 (3) (2022) 1–28.
- [2] A. Alam, S.M.Zur Rashid, Md.A Salam, A. Islam, Towards Blockchain-Based E-voting System, in: *International Conference on Innovations in Science, Engineering and Technology (ICISSET)*, 2018. ISBN: 978-1-5386-8524-2.
- [3] R. Hanifatunnisa, B. Rahardjo, Blockchain based e-voting recording system design, in: *11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1–6.
- [4] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A.K. Bashir, R. Nawaz, Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation, *IEEe Trans. Ind. Appl.* 56 (4) (2019) 4478–4488.
- [5] Y. Dalvi, S. Jaiswal, P. Sharma, E-Voting using Blockchain, *Int. J. Eng. Res.Technol. (IJERT)* 10 (03) (2021).
- [6] G. Rathee, R. Iqbal, O. Waqar, A.K. Bashir, On the Design and Implementation of a Blockchain Enabled E-voting application within IoT-Oriented smart cities, *IEEe Access.* 9 (2021) 34165–34176. Feb.
- [7] M. Pawlak, A. Poniszewska-Mara«da, N. Kryvinska, Towards the intelligent agents for blockchain e-voting system, *Proc. Comput. Sci.* 141 (2018) 239–246. Jan.
- [8] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, P. Vora, Scantegrity: end-to-End voter verifiable optical-scan voting, *IEEE Secur. Privacy* 6 (3) (2008) 40–46. Jun.
- [9] S. Desai, M. Han, L. Li, Z. Li, J. He, X. Xu, ‘Untampered Electronic Voting in Entertainment Industry: a blockchain-based implementation, in: *20th Annual SIG Conf. Inf. Technol. Educ., New York, NY, USA, 2019*, p. 166. Sep.
- [10] A.A. Monrat, O. Schel‘en, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, *IEEe Access.* 7 (2019) 117134–117151. Aug.
- [11] T.A Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: problems and recommendations, *IEEe Access.* 7 (2019) 176838–176869. Dec.
- [12] W. Gao, W. Hatcher, W. Yu, ‘A survey of Blockchain: techniques, Applications, and Challenges, in: *27th International Conference on Computer Communication Networks (ICCCN)*, 2018, pp. 1–11. Jul.
- [13] F. Hao, M.N. Kreeger, B. Randell, D. Clarke, S.F. Shahandashti, P.H.J. Lee, Every vote counts: ensuring integrity in large-scale

- electronic voting, *USENIX J. Election Technol. Syst.* 2 (3) (2014) 1–25. July.
- [14] F. Shahandashti Siamak, H. Feng, DRE-ip: a verifiable e-voting scheme without tallying authorities, in: 21st European symposium on research in computer security, 2016, pp. 223–240. Sep.
- [15] J. Al-Jaroodi, N. Mohamed, Blockchain in Industries: a survey, *IEEe Access.* 7 (2019) 36500–36515. Feb.
- [16] H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for Internet of Things: a survey, *IEEe Internet. Things. J.* 6 (5) (2019) 8076–8094. Oct.
- [17] K. Wüst, A. Gervais, Do you need a blockchain? *Crypto Valley Conf. Blockchain Technol. (CVCBT)* (2018) 45–54. Jun.
- [18] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for Industry 4.0: a comprehensive review, *IEEe Access.* 8 (2020) 79764–79800. Mar.
- [19] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, *IEEe Access.* 7 (2019) 77894–77904. Jun.
- [20] F. Rabia, A. Sara, T. Gadi, A survey on e-voting based on blockchain, in: 4<sup>th</sup> International Conference Netw., *Inf. Syst. Acad. Manage. Perspect. Security*, Apr. 2021, pp. 1–8.
- [21] M.A. Cheema, N. Ashraf, A. Aftab, H.K. Qureshi, M. Kazim, A.T. Azar, Machine learning with blockchain for secure E-voting system, in: 1st International Conference of Smart System and Emerging Technology (SMARTTECH), 2020, pp. 177–182.
- [22] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: *IEEE International Congress on Big Data*, 2017, pp. 557–564. Jun.
- [23] M. Alharby, A. Aldweesh and A.V. Moorsel, “Blockchain-based smart contracts: a systematic mapping study of Academic Research” Sep. 2020.
- [24] M.H. Nasir, M. Imran, J.S. Yang, Study on E-voting systems: a blockchain based approach, in: *IEEE International Conference Consumer Electronics- Asia (ICCE-Asia)*, 2021, pp. 1–4. Nov.
- [25] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, M. Badra, Analysis of blockchain solutions for E-voting: a systematic literature review, *IEEe Access.* 10 (2022) 70746–70759. Jan.
- [26] B. Ahn, Implementation and early adoption of an Ethereum-based electronic voting system for the prevention of fraudulent voting, *Sustainability.* 14 (5) (2022) 2917. Mar.
- [27] J. Goyal, M. Ahmed, D. Gopalani, A privacy preserving E-voting system with two-phase verification based on Ethereum blockchain, *Res. Sq.* (2022) 1–33. Jun.
- [28] K.L. Ohammah, S. Thomas, A. Obadiah, S. Mohammed, Y.S. Lolo, ‘A survey on electronic voting on blockchain, in: *Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technol. Sustain. Develop. (NIGERCON)*, 2022, pp. 1–4. Apr.
- [29] M.V. Vladucu, Z. Dong, J. Medina, R. Rojas-Cessa, E-voting meets blockchain: a survey, *IEEe Access.* 11 (2023) 23293–23308, <https://doi.org/10.1109/ACCESS.2023.3253682>.
- [30] S. Panja, B. Roy, A secure end-to-end verifiable e-voting system using blockchain and cloud server, *J. Inf. Secur. Appl.* 59 (2021) 102815. ISSN 2214-2126 Jun.
- [31] S.S. Hossain, S.A. Arani, M.T. Rahman, T. Bhuiyan, D. Alam, M. Zaman, E-voting system using blockchain technology, in: *Proc. 2nd Int. Conf. Blockchain Technology and Applications*, 2019, pp. 113–117. Dec.
- [32] F.P. Hj’ almarsson, G.K. Hrei’ oarsson, M. Hamdaqqa, and G. Hj’ almtýsson, “Blockchain-based E-voting system”, in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, pp.983986.
- [33] P. McCorry, S. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy. *Financial Cryptography and Data Security*, Springer, Sliema, Malta, 2017, pp. 357–375.
- [34] M. Kumar, S. Chand, C.P. Katti, A secure end-to-end verifiable internet-voting system using identity-based blind signature, *IEEe Syst. J.* 14 (2) (2020) 2032–2041.
- [35] H. Yi, Securing e-voting based on blockchain in P2P network, *EURASIP. J. Wirel. Commun. Netw.* (137) (2019). May.
- [36] S. Panja, S. Bag, F. Hao, Bi. Roy, Smart contract system for decentralized borda count voting, *IEEE Trans. Eng. Manage.* (2020). May.
- [37] F’ D. Giraldo, MC. Barbosa, yCE. Gamboa, Electronic voting using blockchain and smart contracts: proof of concept, *IEEE Latin America Trans.* 18 (10) (2020). Oct.

- [38] M.S. Farooq, U. Iftikhar, A. Khelifi, A framework to make voting system transparent using blockchain technology, *IEEE Access*. 10 (2022) 59959–59969.
- [39] K. Divya, K. Usha, Blockvoting: an online voting system using block chain, in: *Int. Conf. Innovative Trends in Information Technology (ICITIIT)*, 2022, pp. 1–7. Feb.
- [40] M. Malkawi, M.B. Yassein, A. Bataineh, ‘Blockchain based voting system for Jordan parliament elections, *Int. J. Electr. Comput. Eng.* 11 (2021) 4325–4335. Oct. *Journal of Safety Science and Resilience* 5 (2024) 102–109
- [41] S. Panja, Zero-knowledge proof, deniability and their applications in blockchain, E-voting and deniable secret handshake protocols, *Diss. Indian Stat. Inst.-Kolkata* (2021).
- [42] K.M. Khan, J. Arshad, M.M. Khan, Secure digital voting system based on blockchain technology, *Int. J. Electron. Gov. Res.* 14 (1) (2018) 53–62. Jan.
- [43] C. Killer, et al., Provotum: a blockchain-based and end-to-end verifiable remote electronic voting system, in: *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, IEEE, 2020.
- [44] Y. Abuidris, R. Kumar, T. Yang, J. Onginjo, Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding, *Etri J.* 43 (2) (2021) 357–370. Apr.
- [45] S. Suralkar, S. Udasi, S. Gagnani, M. Tekwani, M. Bhatia, E-voting using blockchain with biometric authentication, *Int. J. Res. Analyt. Rev.* 6 (1) (2019) 77–81. Jan.
- [46] K.M. AboSamra, A.A. AbdelHafez, G.M.R. Assassa, M.F.M. Mursi, A practical, secure, and auditable e-voting system, *J. Inf. Secur. Appl.* 36 (2017) 69–89. Oct.
- [47] T. Moura, A. Gomes, ‘Blockchain voting and its effects on election transparency and voter confidence, in: *18th Annual International Conference on Digital Government Research*, New York, NY, USA, 2017, pp. 574–575. Jun.
- [48] S. Zeadally, J.B. Abdo, Blockchain: trends and future opportunities, *Internet Technol. Lett.* 2 (6) (2019) e130. Nov.
- [49] C. Denis Gonz´alez, D. Frias Mena, A. Mass´Mu˜noz, O. Rojas, G. Sosa-G´omez, Electronic voting system using an enterprise blockchain, *Appl. Sci.* 12 (2) (2022) 531.