A SURVEY ON E-VOTING SYSTEMS USING BLOCKCHAIN

Yedhukrishnan V
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
yedhuk0001@gmail.com

Muhammed Udaif P
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
muhammedudaifputhalath@gmail.com

Nanditha V S
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
nandithavs192@gmail.com

Navami K Biju
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
navamy22@gmail.com

Farisa Sali
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
farisasalisana@gmail.com

Linda Sebastian
Dept. of CSE
College of Engineering Kidangoor
Kottayam,India
lindasebastian@ce-kgr.org

Abstract— **In the digital age, traditional voting systems are increasingly facing challenges related to security, transparency, and accessibility. To address these issues, blockchain technology has emerged as a promising solution, offering a decentralized, tamper-proof, and transparent platform for electronic voting. This survey paper provides a comprehensive analysis of the existing literature on blockchain-based e-voting systems, examining the challenges, opportunities, and future directions in this rapidly evolving field. We review different blockchain architectures highlighting their strengths and limitations. Through a systematic examination of existing solutions and case studies, we identify emerging trends and best practices in the design and implementation of blockchain-based e-voting systems.**

Keywords—Blockchain; cryptography; e-voting; smart contracts.

I. INTRODUCTION

Electronic voting (e-voting) refers to the process of casting and counting votes using electronic means, typically through computers or other electronic devices. It offers the potential to streamline the voting process, increase accessibility for voters, and potentially reduce costs associated with traditional paper-based voting systems. However, e-voting also raises concerns about security, privacy, and the possibility of manipulation or hacking. Implementing secure e-voting systems requires robust cybersecurity measures and careful consideration of potential risks and vulnerabilities. In recent years, the integration of blockchain technology into various sectors has sparked considerable interest and innovation. One area where blockchain holds significant promise is in the realm of electoral processes [1]. Campus elections serve as a cornerstone of student governance, empowering students to voice their opinions, elect representatives, and shape the trajectory of their educational experience. However, traditional paper-based voting methods often fail to leverage the full potential of technology, resulting in inefficiencies and limitations that hinder the democratic process. Blockchain-based e-voting systems offer a transformative solution by harnessing the power of decentralization, cryptography, and transparency to revolutionize elections [9]. By providing a secure, tamperproof, and auditable platform for electronic voting, these systems hold the promise of overcoming long standing challenges while fostering greater participation, transparency, and legitimacy in student

democracy. Blockchain-based e- voting systems lie in a decentralized network of nodes, each maintaining a copy of the distributed ledger containing all transactional data related to the electoral process. Through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), these networks validate and record votes in a transparent and immutable manner, preventing tampering or manipulation by malicious actors. Smart contracts, and programmable self-executing protocols deployed on the blockchain, govern the rules and procedures of the voting process, automating tasks such as voter authentication, ballot casting, and result tabulation. Cryptographic techniques, including public-key encryption and digital signatures, ensure the security and privacy of voter data, enabling anonymous yet verifiable participation in elections. Blockchain-based e-voting systems offer a range of potential benefits, including enhanced security, increased transparency, and greater accessibility for voters. By eliminating intermediaries and central points of failure, these systems reduce the risk of fraud and manipulation, thereby fostering trust and confidence in electoral outcomes. Additionally, blockchain technology enables real-time auditing and verification of voting results, allowing stakeholders to independently validate the integrity of the election process. Moreover, e-voting systems can improve voter turnout by providing remote and convenient voting options, particularly for individuals with mobility or accessibility constraints

II. Motivation

Existing voting systems are susceptible to fraudulent attempts, inefficiencies, scalability, and lack of accessibility. To address these issues, there is a need to develop and implement e-voting systems that provide secure, transparent, and verifiable mechanisms to ensure the integrity of the voting process. The system using Blockchain provides a decentralized and tamper-resistant platform for recording and verifying votes. Each vote is encrypted and stored in a series of blocks, forming a chain that is distributed across multiple computers or nodes. This makes it extremely difficult for any single entity to manipulate the results without detection. Additionally, it ensures that once a vote is recorded, it cannot be altered or deleted. This creates an auditable trail, allowing for greater transparency and accountability in the voting process. Anyone with access to the blockchain can verify the legitimacy of the votes, ensuring that the results are accurate and trustworthy. Also, voters can securely cast their votes from anywhere using their smartphones or dedicated voting machines. This eliminates the need for physical presence at polling stations, saving time and resources. Overall, this method provides a secure, transparent, and efficient voting process.

III. Literature Survey

Significant progress has already been achieved in this field, serving as a reference point to understand the foundational ideas and grasp the essential concepts needed for this study.

[1] Introduces an electronic voting system based on blockchain technology. It works by storing the voting data in a decentralized and interconnected manner. Each vote is recorded as a block with a unique code, and the blocks are linked together to form a chain. Figure 1 shows the workflow of the model. SHA- 256 is utilized to create unique hash codes for each block of information related to the voting transactions. These hash codes are then used to link the blocks together, forming a secure and tamper-evident chain. The significance of SHA-256 lies in its ability to provide a high level of security, making it extremely difficult for unauthorized parties to tamper with voting data.

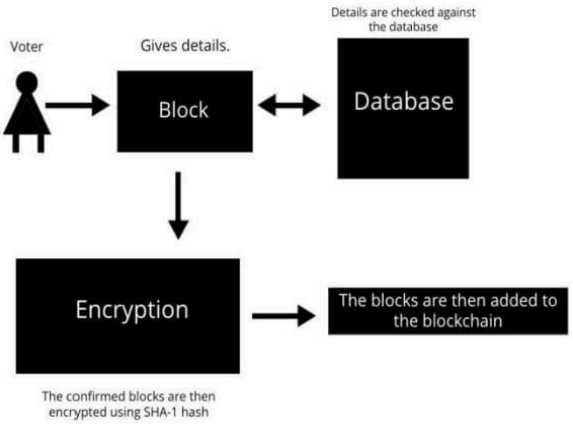

Fig. 1. Workflow of E-voting system [1]

[2] Presented a Secure E-Voting System based on Blockchain technology and authentication via Face Recognition and Mobile OTP. The e-voting system will authenticate users with Aadhaar, verify faces, and use mobile OTP for added security. Votes will be stored securely on a blockchain, ensuring tamper-proof data. Admins can manage candidates and smart contracts on the blockchain prevent

multiple voting. The system aims for transparent and secure national elections.

[3] This paper presents an E-voting system that includes I-Voting (Internet Voting) and SMS-Voting. During registration, users provide their mobile number which is linked to a central database. A one-time password (OTP) is sent to the mobile number for verification. After entering the OTP, face recognition is used to match the user's data with the database.

[4] The widespread use of electronic voting (e-voting) systems as a replacement for traditional elections presents challenges in terms of result confidence. These systems are vulnerable to administrative issues, such as hacking or manipulation by election companies. Centralized internet-based systems, where a single party controls and stores information, raise trust concerns. However, publishing information on a network system can address these problems. Blockchain, a distributed ledger that provides a shared and immutable source of information, offers an ideal solution for electronic voting. This work introduces blockchain-based electronic voting using Ethereum and Meta-Mask. It demonstrates that electronic elections adhere to six key electoral principles, including secret ballot, one person one vote, transparency, accuracy of ballot papers, vote recording and counting, and reliability. Additionally, the evaluation of electronic voting effectiveness revealed that the Gas delay option yielded the best results in terms of the second outcome.

[5] This study provides an overview of blockchain-based voting and its potential to improve electronic voting systems. It discusses the gaps in current electronic voting and explores the benefits and challenges of using blockchain technology. An architectural overview of the mentioned model is given in figure 2. The transparency and security of blockchain-based voting are highlighted and scalability issues and the need for further testing are also mentioned. The study emphasizes the importance of discussing these issues in real voting scenarios and suggests starting with small test centers before expanding. Figure 3 shows the usage rate of the framework. It concludes that while blockchain technology shows promise, it is still in its early stages for electronic voting solutions.

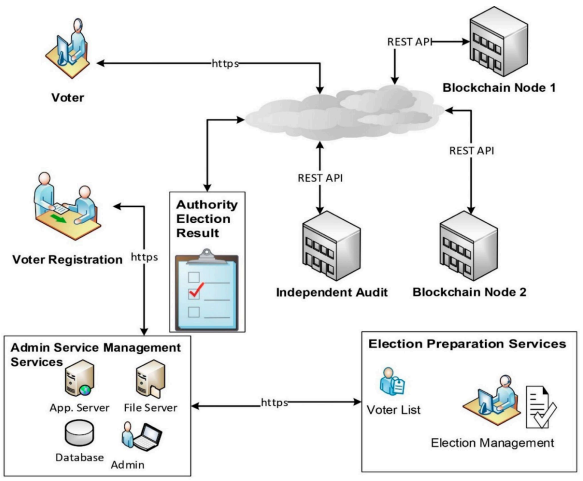

Fig. 2. A Blockchain Voting System Architectural Overview [5]

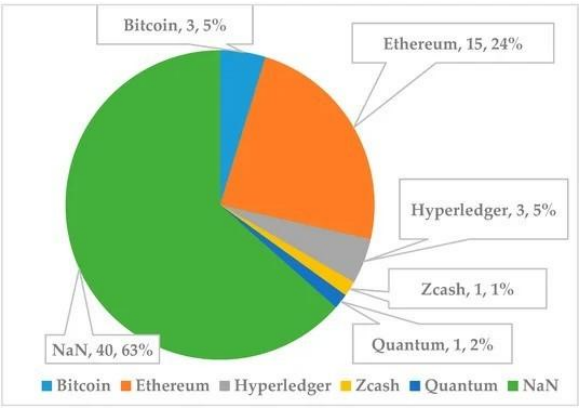

Fig. 3. Blockchain Framework Usage Rate Diagram [5]

[6] This paper describes the use of the signature ring to ensure anonymity in electronic voting. Unlike standard signature algorithms that allow you to verify the identity of the signer, ring signatures allow you to hide your true public key so that the public keys of other participants in the system can be verified. At the same time, blockchain technology can be used to verify the integrity of the user's votes, verify their authenticity (determine the importance of public use), vote counting, and verify the accuracy of votes. The voting record is verified by the user.

[7] The proposed e-voting system introduces a multimodal approach, utilizing fingerprint, facial, and OTP verification to address the limitations of conventional methods and enhance security. By

harnessing the unique strengths of each biometric modality, the system ensures both accuracy and the ability to detect liveness, while also integrating secure communication protocols, biometric template protection, and tamper-proof data storage to safeguard sensitive voter information and privacy. Despite its potential for heightened security and improved voter experience, it remains crucial to tackle concerns regarding privacy, biometric accuracy, and the practical challenges associated with implementation before widespread adoption can be considered. Electronic voting systems must address various issues such as identity, data confidentiality and integrity, transparency.

[8] In the second decade of the 21st century, blockchain emerged as one of the most prominent computational technologies. This study aims to assess the feasibility and suitability of integrating blockchain technology into e-voting systems, considering both technical and non-technical factors. While the adoption of e-voting has been relatively slow, several countries have already implemented such systems for various social and economic reasons, which they have thoroughly examined. However, many countries offer a wide range of e-government solutions beyond e-voting. Given the critical nature of voting in governmental processes, e-voting systems require meticulous attention to potential security and anonymity issues. Nonetheless, e-voting extends beyond governmental services, as many companies and non-profit organizations could benefit from its cost-efficiency, scalability, remote accessibility, and user-friendliness. Blockchain technology is touted as a solution to address some key security concerns, including anonymity, confidentiality, integrity, and non-repudiation. The analysis findings presented in this article largely support these assertions.

[9] In this research paper, the focus is on examining the possibilities of blockchain technology in constructing a decentralized electronic voting (e-voting) system. The study delves deep into the obstacles encountered by conventional centralized e-voting systems, including security weaknesses and a deficiency in transparency. It suggests harnessing blockchain technology to tackle these challenges effectively and establish a voting process that is more secure and transparent.

[10] The paper introduces an electronic voting system utilizing Ethereum's Blockchain technology to overcome issues in centralized voting systems. As shown in figure 4, the approach suggest a decentralized voting application utilizing a smart contract, deploying this smart contract onto a local blockchain network, and creating a dependable, secure, and adaptable electronic voting system that guarantees the accuracy of votes, prevents duplicate voting, and facilitates real-time services. It demonstrates how Blockchain ensures data security in a decentralized manner. The application utilizes Ethereum Blockchain for storing voter accounts, votes, and candidate details, enhancing reliability and preventing duplicate voting. The system allows voters to select candidates via a user-friendly interface, with real-time election result updates.

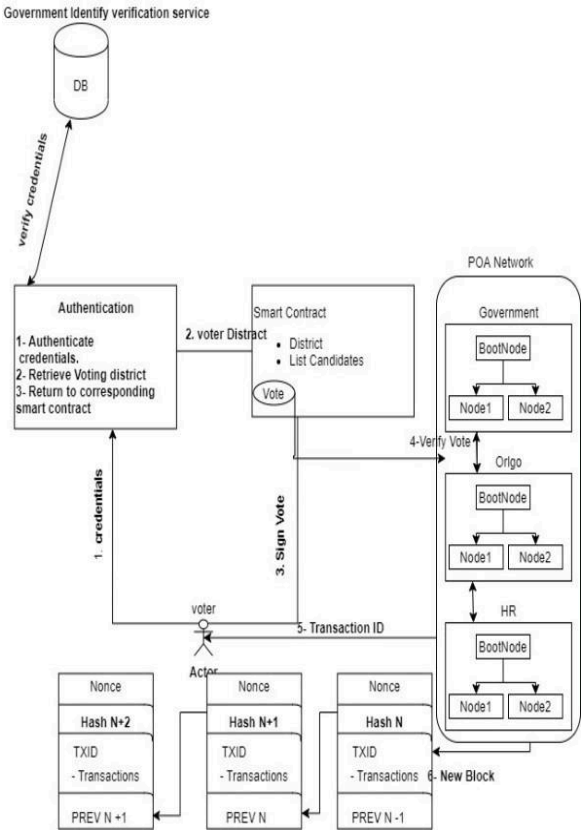

Fig. 4. Process of E-voting.[10]

[11] The paper introduces a decentralized application (DAPP) intended for electronic voting (E-voting) utilizing blockchain technology. It employs decentralized blockchain networks and smart contracts to enhance the security, transparency, and effectiveness of the voting process. The DAPP encompasses the creation of smart contracts to oversee voting procedures, securely log votes on the blockchain, and ensure the integrity of voting data.

The article discusses the planning, execution, and examination of the DAPP prototype, aiming to tackle challenges encountered in traditional E-voting systems such as fraud, manipulation, and a lack of transparency. Overall, the paper contributes to advancing secure and transparent E-voting solutions through the adoption of blockchain technology. Figure 5 depicts the functioning of a decentralized voting application.

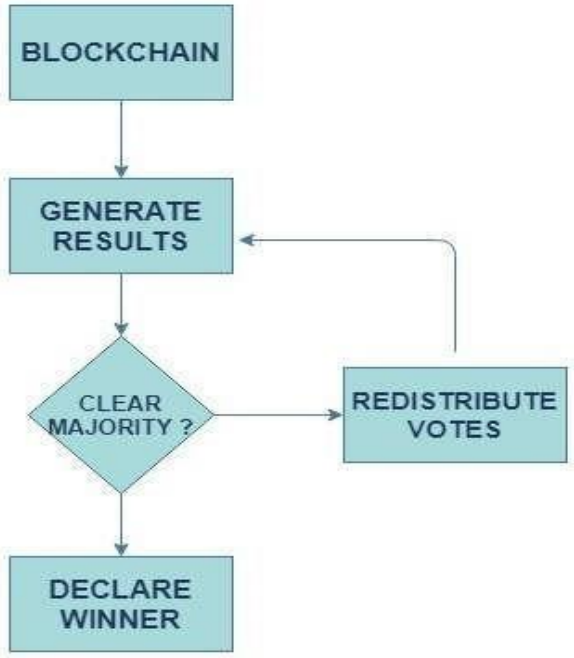

Fig. 5. System flowchart for generating results [12]

[12] The paper suggests a preferential e-voting system based on blockchain technology, utilizing Ethereum's decentralized platform. It tackles the issue of determining a clear majority in elections by introducing a vote-trading mechanism, which redistributes votes among candidates if no decisive majority is reached. This approach provides flexibility as organizations can define their own criteria for determining a majority. The system is developed using the Solidity programming language, allowing voters to prioritize candidates instead of casting a single vote per candidate. It employs preferential voting methods and cryptographic techniques to bolster the integrity of the voting process, aiming to mitigate concerns like tampering, fraud, and coercion commonly linked with conventional voting systems.

TABLE I. COMPARISON

Paper	*Advantages*	*Disadvantages*
Blockchain Based E-voting [1]. 2022	Security: The system ensures the security of votes by introducing a seemingly impenetrable system, making it difficult for unauthorized access or tampering. Anonymity: Voters are provided with anonymity while voting, which encourages more people to participate in the voting process.	Need for a more robust encryption algorithm. Immature practice and technical evolution required before it can be used for national elections due to its energy consumption for authentication and validation.
Secure E-voting System using Blockchain technology and authentication via Face recognition and Mobile OTP [2]. 2021	User Authentication: Aadhaar, face recognition, OTP verify voters securely. Scalability and: Aims for scalable national voting convenience.	Scalability Issues: Potential system failure with high simultaneous votes. Internet Connectivity: Poor connectivity can hinder remote voting.
E-voting system using facial recognition [3]. 2022	Enhanced Security: Deep learning techniques like facial recognition using Convolutional Neural Networks (CNN) can bolster security by verifying voters' identities accurately, reducing the risk of fraudulent activities. Safety Measures: The integration of deep learning can ensure that only eligible voters participate, enhancing the safety of the online voting system.	Validation Challenges: Implementing deep learning requires stringent validation and verification processes to maintain the accuracy and reliability of the facial recognition system, which can be a challenging task. Complex Integration: While blockchain technology offers security benefits, integrating it into the voting process may pose complexities.
Implementation and Evaluation of blockchain-based e-voting systems with	Trust and Transparency: Every participant in the network has access to the same immutable ledger, reducing the risk of manipulation or fraud.	User Adoption: Transitioning from traditional voting systems to blockchain-based e-voting may face resistance from

Paper	*Advantages*	*Disadvantages*
Ethereum and MetaMask [4]. 2020	Fulfillment of Basic Election Principles: The proposed e-voting system fulfills essential principles of an election system, including secret ballot, one-man one-vote, voter eligibility, transparency, accuracy in vote recording and counting, and reliability.	voters who are unfamiliar with blockchain technology. Regulatory Challenges: The legal and regulatory framework surrounding e-voting, particularly on blockchain, is still evolving
A Systematic Review of Challenges and Opportunities of Blockchain for E- Voting [5]. 2020	Comprehensive Review: Covering a wide range of research papers and identifying common challenges and opportunities in the field. Forecasting Future Directions: By analyzing current research, the study aims to forecast future directions in blockchain-based e-voting.	Limited Scope: While the study reviews 63 research papers, the scope may still be limited compared to the vast landscape of blockchain-based e-voting research. Generalization: The study categorizes prevailing issues into five main categories. Some issues may fall outside these predefined categories, leading to potential oversights.
Using Ring Signatures for an Anonymous E-Voting System [6]. 2019	Decentralization: By leveraging blockchain technology, the e-voting system benefits from decentralization, eliminating the need for a central authority and reducing the risk of manipulation or fraud. Integrity and Authenticity: The use of blockchain technology ensures the integrity and authenticity of votes, as each transaction is recorded on the immutable ledger, making it tamper-resistant and verifiable.	Regulatory Challenges: The use of decentralized e-voting systems may raise regulatory concerns, particularly regarding compliance with electoral laws and regulations. Complexity: Implementing ring signatures and blockchain technology in an e-voting system can be complex and require a high level of technical expertise.
Smart voting using Fingerprint , Face and OTP Technology with Blockchain [7]. 2021	Liveness Detection: The system's ability to detect liveness ensures that only live individuals are allowed to cast their votes, preventing spoofing or impersonation attempts. Privacy Protection: Incorporating secure communication protocols, biometric template protection, and tamper-proof data storage helps safeguard sensitive voter information and ensures voter privacy is maintained throughout the voting process.	Complexity: Implementing and managing a system that integrates multiple biometric modalities and security protocols can be complex and require specialized expertise. Cost: Developing, deploying, and maintaining a sophisticated e-voting system with multiple biometric verification methods can be expensive.
A survey on feasibility and suitability of blockchain techniques for the e-voting systems [8]. 2018	Comprehensive Analysis: The study provides a thorough examination of the feasibility and suitability of integrating blockchain technology into e-voting systems, considering both technical and non-technical factors. Blockchain Technology Assessment: The study evaluates blockchain technology as a solution to address key security concerns in e-voting.	Limited Scope: The study focuses primarily on assessing the feasibility and suitability of blockchain technology for e-voting systems, potentially overlooking other important considerations . Limited Discussion on Non-Technical Factors: considering non-technical factors in e-voting system integration, such as social and economic reasons for adoption, it provides limited discussion or analysis on these aspects.
A study on decentralized e-voting systems using blockchain technology [9]. 2018	Highlights the potential benefits of implementing a decentralized e-voting system using blockchain technology such as Transparency and Auditability, Trust and Legitimacy, and Enhanced Security.	Concerns about scalability, complexity, accessibility (especially for voters with limited technological proficiency), and susceptibility to certain types of attacks such as 51% attacks or vulnerabilities in the smart contracts.
Decentralized E-voting system based on Smart Contract by using Blockchain	Proposing a decentralized e-voting system that utilizes smart contracts and blockchain technology. This approach offers increased transparency, security, and reliability compared to traditional	Potential limitations could include a lack of real-world implementation or testing of the proposed system, the need for further validation of the

Paper	*Advantages*	*Disadvantages*
Technology [10]. 2020	centralized voting systems.	effectiveness and security of the approach, and challenges related to scalability and user adoption.
Decentralized Application (DAPP) to enable E-voting systems using Blockchain Technology [11]. 2022	The paper provides insights into the design, implementation, and testing of the DAPP prototype, contributing to the advancement of secure and transparent E-voting solutions.	It may not thoroughly address challenges such as scalability issues, regulatory concerns, or accessibility barriers that could arise from adopting blockchain-based E-voting solutions.
Blockchain-based Preferential E-Voting System DApp using Smart Contract [12]. 2021	The incorporation of a vote-trading mechanism allows for greater flexibility in determining election outcomes, while the utilization of the Solidity programming language enables voters to prioritize candidates, thereby enhancing the integrity of the entire voting process.	Potential drawbacks include the complexity and scalability issues inherent in blockchain technology, particularly in managing large-scale voting scenarios.

IV. METHODOLOGY

Designing a blockchain-based decentralized campus e- voting application involves careful planning and consideration of various factors. Below is a methodology to guide you through the development process [3]:

A. Define Objectives and Requirements:

1. Identify Stakeholders: List all stakeholders involved, including administrators, students, faculty, and any other relevant parties.
2. Specify Functional Requirements: Define the features and functionalities required, such as user registration, candidate nomination, voting, and result publication.
3. Outline Non-functional Requirements: Address scalability, security, privacy, and usability concerns. Specify performance metrics, such as transaction processing speed and system availability.

B. Choose Blockchain Technology:

1. Select a Suitable Blockchain Platform: Evaluate various blockchain platforms (e.g., Ethereum, Hyperledger, or others) based on the project requirements.

C. Architecture and Design:

1. Design Smart Contracts: Develop smart contracts for user registration, voting, and result verification. Implement security measures to prevent vulnerabilities.
2. Define User Roles: Clearly define the roles and permissions of administrators and users.
3. Implement Privacy Measures: Integrate privacy features like zero-knowledge proofs to protect voter anonymity.Integrate face recognition-based login for advanced security.
4. User Interface Design: Develop a user-friendly interface for both administrators and voters.

D. Security Measures:

1. Encryption: Implement end-to-end encryption for communication between nodes and users.
2. Access Control: Apply robust access controls to ensure only authorized users can perform specific actions.
3. Threat Modeling: Identify potential security threats and vulnerabilities and develop countermeasures.

E. Development:

1. Smart Contract Development: Code and test smart contracts on the chosen blockchain platform.
2. Front-end and Back-end Development: Develop the user interfaces and backend systems for the application.
3. Integration: Integrate the front-end, back-end, and smart contracts into a cohesive system.

F. Testing:

1. Unit Testing: Conduct thorough unit testing for each component of the application.
2. Integration Testing: Verify the interoperability of different modules.
3. Security Testing: Perform penetration testing to identify and address potential security vulnerabilities.

V. Conclusion

In conclusion, this survey has provided a comprehensive overview of blockchain-based e-voting systems, highlighting their potential to address the challenges associated with traditional voting mechanisms while introducing new opportunities for transparency, security, and efficiency. We have explored various blockchain architectures and implementation approaches used in e-voting systems, emphasizing their strengths and limitations. Despite the promising features offered by blockchain technology, several challenges remain to be addressed. Security and privacy concerns, scalability issues, and usability challenges pose significant barriers to the widespread adoption of blockchain-based e-voting systems. Moreover, regulatory and legal frameworks need to be developed to ensure compliance and trust in these systems.

The scope of the survey is on the feasibility and suitability of blockchain techniques for e-voting systems that could include several avenues for further research and development such as to address specific requirements and challenges of e-voting systems, like scalability, throughput, privacy, and interoperability, to make them more suitable for large-scale electoral processes and enhancing the security features of blockchain protocols. This mitigates threats such as double voting, manipulation of voting data, denial-of-service attacks, and collusion among malicious actors, thereby ensuring the integrity and trustworthiness of e-voting systems. E-voting using blockchain offers several potential advantages which includes secure, transparent, and tamper-proof voting processes while preserving voter anonymity, eliminating the need for intermediaries, and automating execution, thus enhancing efficiency and trust in electoral systems. Overall, e-voting with blockchain holds promise for improving the efficiency, trustworthiness, and accessibility of electoral processes.

References

[1] Kabra, Palak Pannu, Gurleen Kaushik, Shrinjay Pimple, Aaryan. “Blockchain Based E-Voting.” International Research Journal of Engineering and Technology ,2022

[2] Parmar, Abhishek, et al. "Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[3] Domakonda, Sreekanth Kumar, Arigala Rao, Alladi Sindhu, Ankammagari et al. “E-Voting System Using Facial Recognition.” The International journal of analytical and experimental modal analysis, 2022.

[4] Pramulia, Deni, and Bayu Anggorojati. "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask." 2020 international conference on informatics, multimedia, cyber and information systems (ICIMCIS). IEEE, 2020.

[5] Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." Symmetry 12.8 (2020): 1328.

[6] Kurbatov, Oleksandr, et al. "Using ring signatures for an anonymous e-voting system." 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). IEEE, 2019.

[7] P. Katta, O. A. Mohammed, K. Prabaakaran, M. Divya, G. Jayashree, and D. Keerthika, "Smart voting using Fingerprint, Face and OTP Technology with Blockchain," Journal of Physics: Conference Series, vol. 1916, no. 1, p. 012139, 2021. DOI: 10.1088/1742-6596/1916/1/012139.

[8] Çabuk, Umut Can, Eylul Adiguzel, and Enis Karaarslan. "A survey on feasibility and suitability of blockchain techniques for the e-voting systems." arXiv preprint arXiv:2002.07175 (2020).

[9] Patil, Harsha V., Kanchan G. Rathi, and Malati V. Tribhuwan. "A study on decentralized e-voting systems using blockchain technology." Int. Res. J. Eng. Technol 5.11 (2018): 48-53.

[10] Al-Madani, Ali Mansour, et al. "Decentralized E-voting system based on Smart Contract by using Blockchain Technology." 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC). IEEE, 2020.

[11] Garg, Harshita, et al. "Decentralized Application (DAPP) to enable E-voting systems using Blockchain Technology." 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA). IEEE, 2022.

[12] Gupta, Saurav, and Manjunath CR. "Blockchain-based Preferential E-Voting System DApp using Smart Contract." Proceedings of the International Conference on Innovative Computing & Communication (ICICC). 2021.