IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain based safe Electronic Voting System

Prof. Manjunath T N
Associate Professor, Dept of CSE.
East West Institute of Technology
Bengaluru, India

Tejushree R P
Dept of CSE
East West Institute of Technology
Bengaluru, India

Abstract: Abstention rates are still rising today, partly because voters must travel to cast their ballots. For this reason, everyone will be able to vote remotely via electronic voting, increasing turnout by eliminating the need for travel. In addition, it will yield results more quickly and with less risk than a typical paper ballot vote. The advantages that these systems offer, such as the ability to vote remotely and expedited vote counting, can be used to explain this tendency. In fact, a remote e-voting system needs to be the best in terms of security, dependability, and transparency because elections carry such high stakes. Only then can citizens trust such a system. The immutable vote storage mechanism of blockchain technology increases the voting process's resilience, lowering the possibility of vote tampering and preserving the validity of elections. Several nations, including Germany, Russia, Estonia, and Switzerland, have included this technology into their electronic voting systems. This paper offers a thorough analysis of the blockchain-based electronic voting methods that are being adopted by numerous nations and businesses and that have been suggested for scholarly investigation.

INDEX TERMS

Blockchain, Electronic voting, Authentication, Privacy, Security, Transparency.

I. INTRODUCTION

Voting and elections are essential in today's democratic environment. Voters would value the ability to cast their ballots from any location, making electronic online voting via the Internet even more lucrative[1]. The process of voting on paper ballots could become more inclusive and accessible with the introduction of electronic voting, or "e-voting"[7]. As the name suggests, electronic voting is a voting procedure conducted through electronic medium. One benefit of electronic voting is that it allows voters to cast their ballots without physically visiting the polling place, and it also makes vote tallying and collection more easy[1]. On the one hand, the requirement to travel in order to cast a ballot has contributed significantly to the rising percentage of voter disengagement. On the other side, electoral transparency is being questioned and attacked more and more in many nations[2]. An internet voting system should satisfy the requirements like Accuracy, Simplicity, Democracy, Verifiability, Privacy and Security. Among these, security and privacy are main concerns. Therefore, it would seem that implementing a safe Internet voting system is another way that network security and cryptography are put to use. Blockchain appears to be a promising technique to overcome these issues[3].

Blockchain is a upcoming technology that has not yet reached its full potential but is developing into ever-more-useful applications[3]. An electronic or online voting node that is decentralized is provided by blockchain technology. Due to the benefits of end-to-end verification, distributed ledger technologies like blockchain have recently been utilized to create electronic voting systems[2]. Our method proposes a workable implementation of the current cryptographic techniques and digital signatures to guarantee the validity of the votes cast by voters and their authentication at both levels. The creation of a safe electronic voting system via a network is undoubtedly a challenging undertaking, as it must fulfill all the necessary specifications. Inadequate adherence to even a single specification may result in weaknesses and errors that an intermediary could utilize to falsify or alter the complex information. As a result, a voting system needs to guarantee that the voter can conceal his vote[15].

Scaling blockchains is still a major difficulty, particularly when handling massive elections with millions of votes and lots of transactions. Maintaining the integrity and confidentiality of the voting process depends on securing blockchain-based electronic voting systems against online threats including hacking, manipulation, and denial-of-service attacks. There is a fine balance to be struck between protecting voter privacy and ensuring voting process openness and auditability, which calls for strong cryptography methods and technologies that enhance privacy. Blockchain-based electronic voting systems must be designed with user-friendly interfaces and simple voting procedures that accommodate voters with different levels of technological expertise if they are to be widely adopted and accepted. Ensuring ballot privacy while maintaining voting accuracy requires systems that allow voters to confirm their votes are cast and counted on the blockchain. This is a

crucial step in maintaining public confidence in the election process.

II.RELATED WORKS

A block is associate degree mass set of information. knowledge square measure collected and methoded to suit in an exceedingly block through a process known as mining. Every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block, during this method, all the information may be connected via a connected list structure[4]. In [9] the researcher proposed an E-voting application with a decentralized database using Blockchain to avoid the drawback of the traditional web application. The purpose of developing E-voting application is to ensure that the vote is counted, all the votes are only kind of once, and the correct candidates with most votes are actually going to win the election. To achieve this purpose the application needs blockchain which provides the decentralized voting application. The use of block chain technology can provide mankind with the best solution to conduct elections in the most secure, transparent, flexible and cost-efficient way. The popularity of blockchain can easily be understood by the fact that this technology is being utilized by many crypto currencies, including bitcoin transaction framework[6]. Blockchain E-voting system help to avoid or minimize fraud during the UTHM Student Representative Council election. The system has successfully developed and comply with the objectives, however, some improvements can be considered in the future for a better system; in terms of practicality and user friendly. With the blockchain technology, it appears that the future is bright and promising[8]. During the voting phase, the smart contracts are initialized with the voting rules, the list of voters and the list of candidates. Any subsequent modification of this phase must be made according to these initial smart contracts. on the day of the election, the users connect and identify themselves thanks to the different authentication mechanisms presented in section IV-B. Sometimes a dedicated website or application is used. once identification is well done, the voter chooses one or several candidates according to the voting rules. The vote is then encrypted using an encryption algorithm or hashed using a hash function. The encrypted or hashed vote is finally added to the blockchain. Indeed, this vote is invisible and irreversible in many cases. when the end of the election is declared, it becomes impossible to change or add votes[3]. The use of hash assures the privacy of voters and the concept of public and private keys allows the authorities to control the process precisely. The traceability of the voting system assists in preventing hackers from modifying or viewing the voting information. It assures that one voter only votes one vote. The usability of this system performs well by using the more effective approach of implementing a flexible consensus algorithm to reduce extensive computing resources in the blockchain. This transparent behavior of the system tends to be promising for voters to rely and trust. The Chain Security Algorithm is also added, which automatically verifies the validity of the chain each time a new block is added to it[12]. If the counting process takes place in parallel with the voting, it is essential that the current score is not visible to anyone to avoid influencing voters who have not yet voted[3]. Electronic voting technology aims to speed up ballot counting, reduce the cost of paying staff to manually count votes, and improve accessibility for disabled voters. In the long term, expenses are expected to decrease. Results can be reported and published faster[10]. The application based on Ethereum Blockchain technology as a network and a decentralized database all in one for storing voter's accounts, votes, and candidates details. Blockchain provides a decentralized model that makes the network reliable, safe, flexible and able to support real-time services. the voter realizes his vote goes to his right candidate as well as he has only one vote because the application does not allow for the duplicate vote by this method electronic voting could be highly reliable[9]. Blockchain appears as an interesting alternative to traditional voting systems. The world of blockchain is a constantly evolving ecosystem, as many are created while others disappear[3]. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain-based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed. Due to these concerns, it was determined that the existing frameworks need to be improved to be utilized in voting systems[2].

III.SYSTEM MODEL

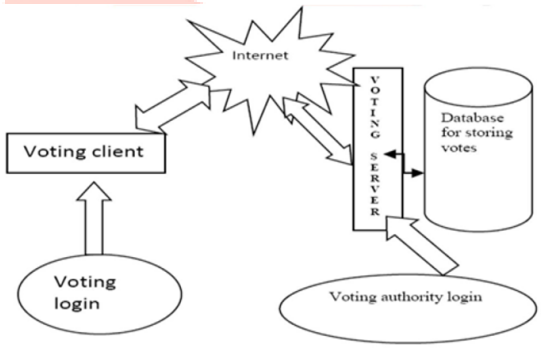

Figure : Computation on client side.

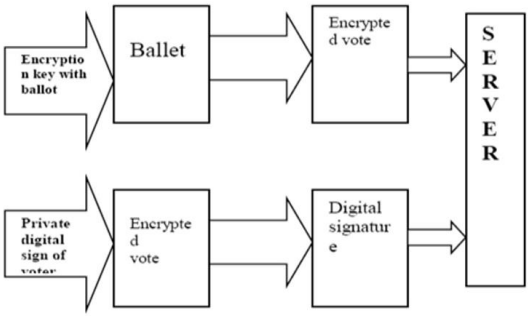

Figure 2 : Voting client side computing

A.IMPLEMENTATION

Implementing an e-voting system using blockchain and face recognition with Django involves several steps. Below is a high-level overview of how you can implement each component: **Setup Django Project:** Create a new Django project using the django-admin command. Set up Django apps for different functionalities such as user management, candidate management, and voting. **User Authentication:** Implement user authentication using Django's built-in authentication system

or custom authentication methods. Include user registration, login, logout functionalities in your Django application. **Face Recognition Integration:** Install necessary libraries such as OpenCV or Dlib for face detection and recognition. Create views in Django to handle user image capture during registration and authentication. Train a machine learning model for face recognition and integrate it with your Django views. **Blockchain Integration:** Choose a blockchain platform or framework suitable for your project (e.g., Ethereum, Hyperledger). Develop smart contracts for managing voting transactions and candidate registration. Integrate your Django backend with the blockchain network using appropriate APIs or SDKs (e.g., Web3 for Ethereum). **Candidate Registration:** Create forms or APIs for candidates to register themselves, providing necessary details and images. Validate and store candidate information in your Django database. **Voting Process:** Design user interfaces for casting votes, displaying candidate profiles, and confirming votes. Implement logic for recording votes in the blockchain using smart contracts. Integrate face recognition during the voting process to authenticate voters. **Result Viewing:** Develop views to display election results, including vote counts for each candidate. Fetch data from the blockchain or database and present it in a user-friendly format. **Security Measures:** Implement encryption mechanisms to secure user data and transactions. Apply security best practices to prevent unauthorized access and tampering with voting data. Regularly update software components to address security vulnerabilities. **Testing and Deployment:** Test the entire system thoroughly, including functionality, security, and performance. Deploy your Django application and blockchain network on suitable hosting platforms or servers. Perform continuous monitoring and maintenance to ensure system reliability and security.

B.METHODOLOGY

Implementing an e-voting system using blockchain and face recognition involves several key steps. Here's a methodology to guide you through the process:

1. Requirement Analysis: Identify the specific requirements of your e-voting system, including user roles, authentication methods, voting process, candidate registration, and result viewing. **2. Choose Technology Stack:** Select appropriate technologies for building the system, such as Django for web development, OpenCV or Dlib for face recognition, and a suitable blockchain platform like Ethereum or Hyperledger for implementing the blockchain component. **3. Design System Architecture:** Design the overall architecture of the e-voting system, including the frontend, backend, database, face recognition module, and blockchain integration layer. Define the interactions between different components and how data flows through the system. **4. User Authentication and Registration:** Implement user authentication mechanisms using Django's authentication system or third-party libraries. Develop user registration functionality, including capturing user details and verifying identities using face recognition during registration. **5. Candidate Registration:** Create a module for candidates to register for elections, providing their details, images, and election platform. Implement validation checks to ensure the authenticity of candidate registrations. **6. Blockchain Integration:** Choose a suitable blockchain platform and set up a blockchain network for storing voting data securely. Develop smart contracts to manage voting transactions, candidate registration, and result recording on the blockchain. Integrate the blockchain network with your Django backend using appropriate APIs or SDKs. **7. Voting Process:** Design user interfaces for casting votes, displaying candidate profiles, and confirming votes. Implement logic for recording votes on the blockchain using smart contracts, ensuring transparency and immutability of voting data. Integrate face recognition during the voting process to authenticate voters before casting their votes. **8. Result Viewing:** Develop views to display election results, including vote counts for each candidate and overall election outcomes. Fetch data from the blockchain or database and present it in a user-friendly format for stakeholders to view. **9. Testing and Quality Assurance:** Test the entire system rigorously to ensure functionality, security, and performance. Conduct unit tests, integration tests, and system tests to validate each component's behavior. Perform security audits to identify and mitigate potential vulnerabilities. **10. Deployment and Maintenance:** Deploy the e-voting system on a suitable hosting platform or server infrastructure. Monitor the system's performance and stability in production environments. Provide ongoing maintenance and support to address any issues and implement updates or enhancements as needed.

IV.CONCLUSION

The new version of e-voting system using blockchain technology will be proposed and developed. The system involves combining the security and transparency of blockchain technology with the accuracy and authentication capabilities of face recognition systems. Blockchain provides a decentralized and immutable ledger that records all transactions or actions in a tamper-resistant manner. The creation of blockchain-based voting systems is becoming more and more popular due to the technology's quick development and acceptance. An overview of blockchain-based, electronic, and conventional voting methods is provided by this survey. The glossary classifies terms used in the introduction and usage of blockchain voting systems, including frameworks, cryptography, consensus algorithms, performance evaluation, and qualities of a successful system. We examine the difficulties blockchain-based electronic voting systems encounter and how the systems under examination resolve them, talk about security and privacy issues, and offer some research ideas for reliable and well-liked electronic voting systems.

REFERENCES

1. Haibo Yi1. “An Efficient E-Voting System for Business Intelligence Innovation Based on Blockchain”. 2023

2. Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina Shukur. “Blockchain for Electronic Voting System—Review and Open Research Challenges”. 2021

3. ALI BENABDALLAH1 , ANTOINE AUDRAS , LOUIS COUDERT , NOUR EL MADHOUN, AND MOHAMAD BADRA. “Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review”. 2022

4. Prof. Anita A. Lahane1,⁎, Junaid Patel1,⁎⁎ , Talif Pathan1,⁎⁎⁎ and Prathmesh Potdar. “Blockchain technology based e-voting system”. 2020
5. Muhammad Asaad Cheema, Nouman Ashraf, Asad Aftab, Hassaan Khaliq Qureshi. “Machine Learning with Blockchain for Secure E-Voting System”. 2020
6. Ritika Singh1 , Riya Chaudhary2 , Adarsh Tripathi. “Electronic Voting System Using Blockchain”. 2021
7. MARIA-VICTORIA, ZIQIAN DONG, JORGE MEDINA3 AND ROBERTO ROJAS-CESSA. “E-Voting Meets Blockchain: A Survey”. 2023
8. Yamuna Rosasooria, Abd Kadir Mahamad, Sharifah Saon, Mohd Anuar Mat Isa, Shingo Yamaguchi, Mohd Anuaruddin Ahmadon. “E-Voting on Blockchain using Solidity Language”. 2020
9. Ali Mansour Al-madani, Dr.Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T.Ahmed. “Decentralized E-voting system based on Smart Contract by using Blockchain Technology”. 2021
10. Anli Sherine, Geno Peter, Albert Alexander Stonier, DesmondWong Leh Ping, K. Praghash and Vivekananda Ganji. “Development of an Efficient and Secured E-Voting Mobile Application Using Android”. 2022
11. Haibo Yi, “Securing e-voting based on blockchain in P2P network”. 2019
12. MUHAMMAD SHOAIB FAROOQ, USMAN IFTIKHAR AND ADEL KHELIFI. “A Framework to Make Voting System Transparent Using Blockchain Technology”. 2022
13. RICARDO LOPES ALMEIDA, FABRIZIO BAIARDI, DAMIANO DI FRANCESCO MAESA AND LAURA RICCI. “Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey”. 2023
14. SIMONA-VASILICA OPREA, ADELA BÂRA, ANCA-IOANA ANDREESCU AND MARIAN POMPILIU CRISTESCU. “Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level”. 2022
15. Jena Catherine Bel.D, Savithra.K , Divya.M. “A Secure Approach for E-Voting Using Encryption and Digital Signature”. 2022
16. Hang, L.; Kim, D.-H. “Design and implementation of an integrated iot blockchain platform for sensing data integrity”. Sensors 2019, 19, 2228..
17. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. “An overview of cyber-physical security of battery management systems and adoption of blockchain technology”. IEEE J. Emerg. Sel. Top. Power Electron. 2020
18. Zhang, L.; Peng, M.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. “Secure and efficient data storage and sharing scheme for blockchain—Based mobile—Edge computing”. Trans. Emerg. Telecommun. Technol.2021.
19. Kumar, D.; Dwivedi, R.K. “Designing a Secure E Voting System Using Blockchain with Efficient Smart Contract and Consensus Mechanism”. In Proceedings of the International Conference on Advanced Network Technologies and Intelligent Computing, Varanasi, India, 22– 24 December 2022; Springer Nature Switzerland: Cham, Switzerland, 2023;pp.452–469.
20. Seo-Il Kang and Im-Yeong Lee “A Study on the Electronic Voting System using blind Signature for Anonymity”, IEEE 2006 International Conference on Hybrid Information Technology (ICHIT'06) 0-7695-2674-8/06
21. Chun-Ta Li, Min-Shiang Hwang , Yan-Chi Lai “A Verifiable Electronic Voting Scheme Over the Internet”,2009 Sixth International Conference on Information Technology: New Generations
22. Lazaros Kyrillidis, Sheila Cobourne, Keith Mayes, Song Dongy and Konstantinos Markantonakis “Distributed e-Voting using the Smart Card Web Server” 978-1-4673-3089-3/12@ 2012 IEEE
23. YousfiSouheib,DerrodeStephane, “Watermarking in e-voting for large scale election”, 978-1- 4673-1520-3/12/$31.00 ©2012 IEEE [9] Prof. Emil Sofron, Prof. Ion Tutanescu, “Anatomy and Types of Attacks against Computer Networks”, 978-1-4673-15203/12/$31.00 ©2012 IEEE