iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59313

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

E-Voting System Using Blockchain

Darshil Raval[1], Ajay Pillai[2], Mit Chauhan[3], Shivani Das[4], Dr. Yassir Farooqui[5]
[1, 2, 3, 4]*Student,* [5]*Assistant Professor, Dept. Computer Science and Engineering, Parul University, Vadodara, India*

Abstract: ***Since the 1970s, electronic voting (e-voting) has evolved, offering efficiency and reduced errors, but faces challenges in security and accessibility. Blockchain technology emerges as a disruptive force with potential to fortify e-voting systems. Voting is fundamental to democracy, yet concerns over reliability and accessibility persist. E-voting, while introduced to address these concerns, remains costly and centralized. Blockchain's decentralized nature holds promise for overcoming these challenges. This study introduces e-Vote, a blockchain- based voting system designed for privacy, accessibility, and security. Leveraging Ethereum's blockchain and smart contracts, e-Vote offers a scalable framework for university level elections. Utilizing cryptographic techniques such as homomorphic encryption, e-Vote ensures voter privacy. Our implementation, tested on Ethereum's Testnet, demonstrates usability, scalability, and efficacy. Successful integration of e-Vote requires two key components: the Election Commission, managing elections and candidates through smart contracts, and the voter's module, enabling individuals to cast ballots for their respective constituencies, with each ballot recorded on the blockchain to prevent tampering.***

I. INTRODUCTION

Voting democratically is fundamental to every nation, but it's time to modernize the process with digital technology. Digital voting, whether through electronic machines at polling stations (e-voting) or web browsers (ivoting), offers conve- nience but raises concerns about security. Blockchain tech- nology, a distributed ledger system, holds promise for rev- olutionizing elections. Features of blockchain-based e-voting systems include secure voter registration, anonymous voting, and verifiable vote counts. The immutability of the blockchain ensures tamperproof results and enhances accessibility by allowing voters to cast their ballots remotely. By leveraging blockchain technology, e-voting systems can address security vulnerabilities and improve the integrity and accessibility of elections, ushering in a new era of democratic participation.

A. Blockchain-Powered Web Application for Secure Remote Voting: Addressing Electoral Integrity and Logistical Challenges

The project's overarching goal is to create a web application harnessing blockchain technology for remote voting, with a core focus on upholding the integrity of the electoral process and mitigating logistical hurdles inherent in traditional polling mechanisms. By capitalizing on the decentralized and tamper- resistant nature of blockchain, the application aims to fortify the security and accuracy of each vote, thereby addressing the vulnerabilities inherent in centralized voting systems prone to hackingand manipulation. Central to this endeavor is the facilitation of remote voting for individuals possessing valid citizenship in their respective countries, thereby democratizing the electoral process and enhancing participation. Moreover, the project seeksto confront critical issues such as data integrity and security, which have been persistent concerns in existing voting systems. In tandem, the initiative endeavors to leverage blockchain's capabilities to streamline the voting process, alleviate the burden associated with physical polling stations, and extend the franchise to non-resident citizens through online platforms. Beyond itsimmediate objectives in the realm of electoral governance, the project also aims to deepen understanding of blockchain principles and explore its versatile applications across a spectrum of industries, thereby catalyzing broader technological innovation and societal advancement.

B. Decentralized Technologies and Blockchain

1) Ethereum: Ethereum is a decentralized blockchain plat- form for running smart contracts, developed by Vitalik Buterin in2013.
2) Smart Contract: Self-executing contracts with terms written into code, allowing for automation of digital contracts on a distributed blockchain network.
3) MetaMask: A Chrome extension serving as an Ethereum browser, enabling users to interact with decentral- ized apps andsmart contracts.
4) ERC20: A common type of token on Ethereum repre- senting fungible assets, often used for value transfer within the ecosystem.
5) IPFS: A distributed file-sharing system used for storing data in a decentralized manner, ensuring data integrity and im- mutability.

©IJRASET: All Rights are Reserved

6) Ether.js: A JavaScript library for interacting with the Ethereum blockchain, used for making transactions and calls to smart contracts.
7) React.js: A JavaScript library for building dynamic user interfaces, suitable for creating responsive interfaces in e- voting systems.

C. Motivation for a Decentralized voting platform

The motivation for a decentralized voting platform stems from the pressing need to address the shortcomings and vulner- abilities inherent in traditional centralized voting systems. Centralized voting systems are susceptible to various forms of ma- nipulation, including hacking, tampering, and fraud, which can undermine the integrity and fairness of elections. Furthermore, centralized systems often lack transparency and accountability, leading to concerns about the accuracy and reliability of electionresults.

By transitioning to a decentralized voting platform, several key benefits can be realized. Firstly, decentralization enhances the security and resilience of the voting process by distributing data across a network of nodes, making it more resistant to tampering and manipulation. Additionally, decentralized platforms can increase transparency and auditability, as all transactionsand operations are recorded on an immutable blockchain ledger, accessible to all stakeholders.

Moreover, decentralized voting platforms promote inclu- sivity and accessibility by enabling remote voting options and eliminating geographical barriers to participation. This can lead to higher voter turnout rates and greater democratic engagementamong citizens.

Furthermore, decentralization fosters trust and confidence in the electoral process by empowering voters with greater control over their own data and ensuring that their votes are counted accurately and securely. By leveraging emerging tech- nologies such as blockchain and cryptography, decentralized voting platforms offer a promising solution to the challenges facing modern electoral systems, paving the way for more transparent, secure, and inclusive democratic processes.

II. SOFTWARE DESIGN & METHODOLOGY

A. Software Design

A project plan is a blueprint for the procedures the project team plans to use to accomplish the project's goals. It combines many crucial elements of this process, such as its scope, timeliness, and related hazards. Between the members of the project team and the reviewers, the project plan may be seen as a kind of "contract".

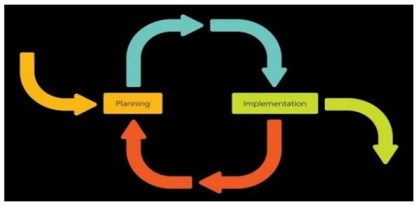


Fig. 1 Iterative model of SDLC

It outlines the steps that will be taken to accomplish the goals as well as who will be responsible for what. It also supports avariety of other crucial project management tasks, such as predicting and estimating, weighing alternatives and making decisions, and controlling and monitoring performance.

B. Process

In the initial phase of development projects, thorough planning is essential to outline specifications, identify software or hard-ware requirements, and prepare for subsequent phases. This phase lays the groundwork for the project's progression. Following the planning phase, an analysis is conducted to determine the appropriate business logic, database models, and other necessary elements. The design stage establishes technological specifications such as programming languages, data layers, and services to fulfill the requirements identified during the analysis. With planning and analysis completed, the implementation and coding processes commence. The first iteration of the project includes all planned, specified, and designed elements that have been coded thus far. After coding and implementing the initial iteration, thorough testing processes are undertaken to identify and ad-dress any defects or issues that may have emerged during development.

Upon completing all preceding phases, a comprehensiveevaluation is conducted to assess project progress. This evaluation enables the project team, along with clients and stakeholders,to review key components such as requirements, scope, schedule, resources, quality criteria, and communication plans.

C. Flowchart

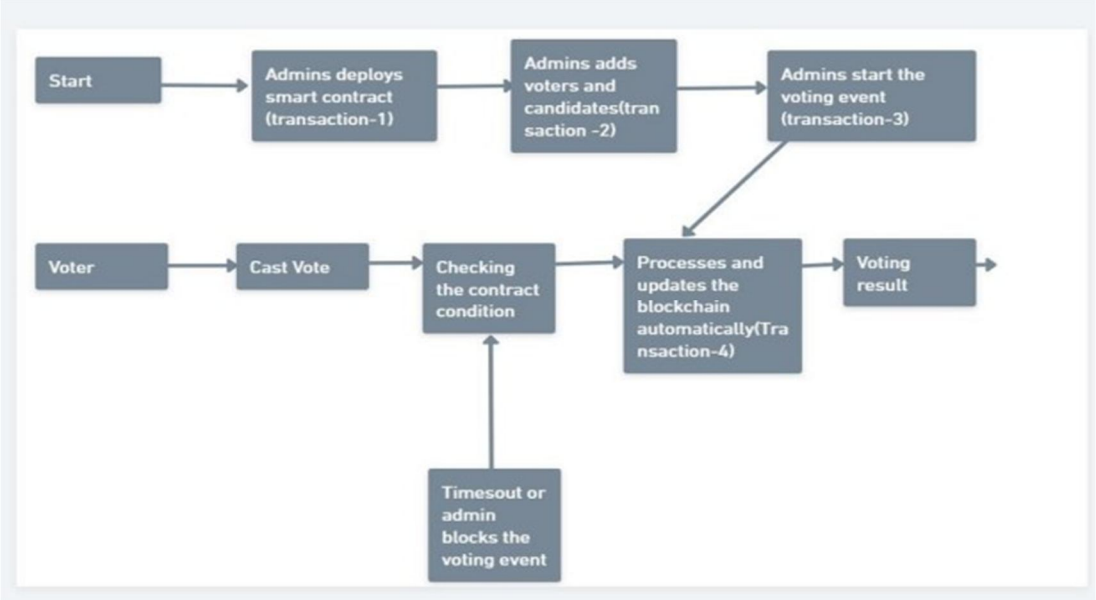


Fig. 2 System Flowchart

1) Admins deploy the smart contract to the blockchain. This transaction creates the contract and makes it available for use.
2) Admins add voters and candidates to the smart contract. This transaction ensures that only eligible voters can participatein the election and that all candidates are properly registered.
3) Admins start the voting event. This transaction opens the election to voters.
4) Voters cast their votes in the smart contract. This transaction updates the blockchain with the voter's selected candidate.
5) The smart contract checks the contract condition. This condition is typically a set amount of time that has passed since the election started. Once the condition is met, the voting event ends and the smart contract automatically processes and updates the blockchain with the results.
6) The voting result is displayed to the public.

III. IMPLEMENTATION

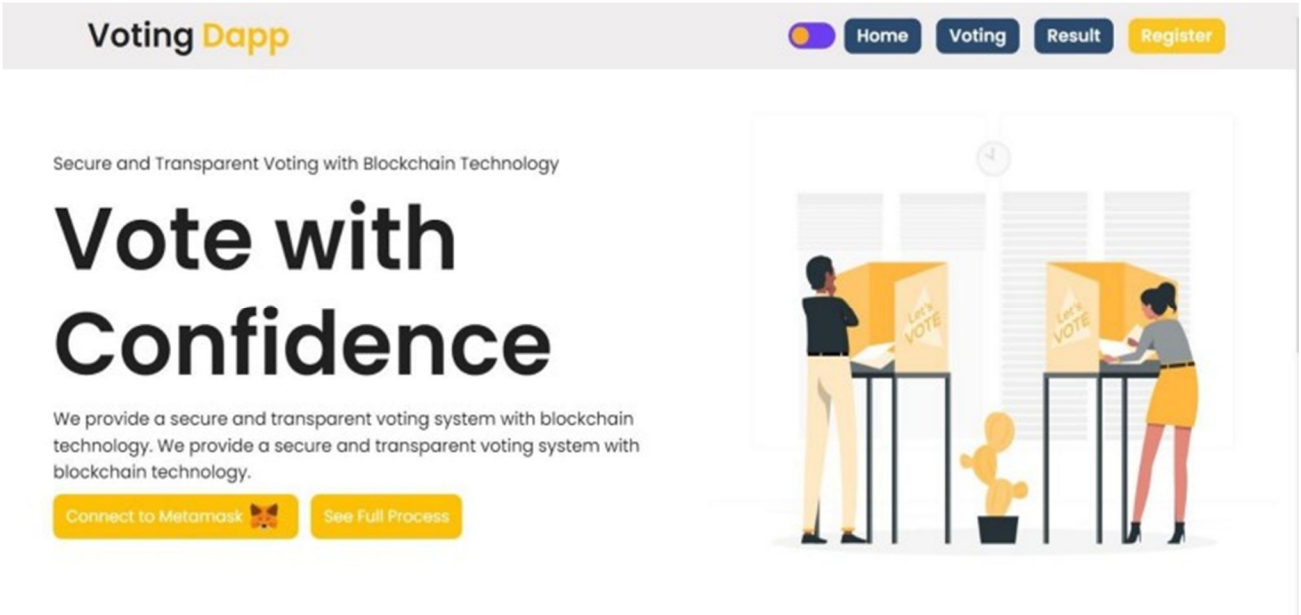


Fig. 3 Home Page

Fig. 4 Admin Page for candidate registering

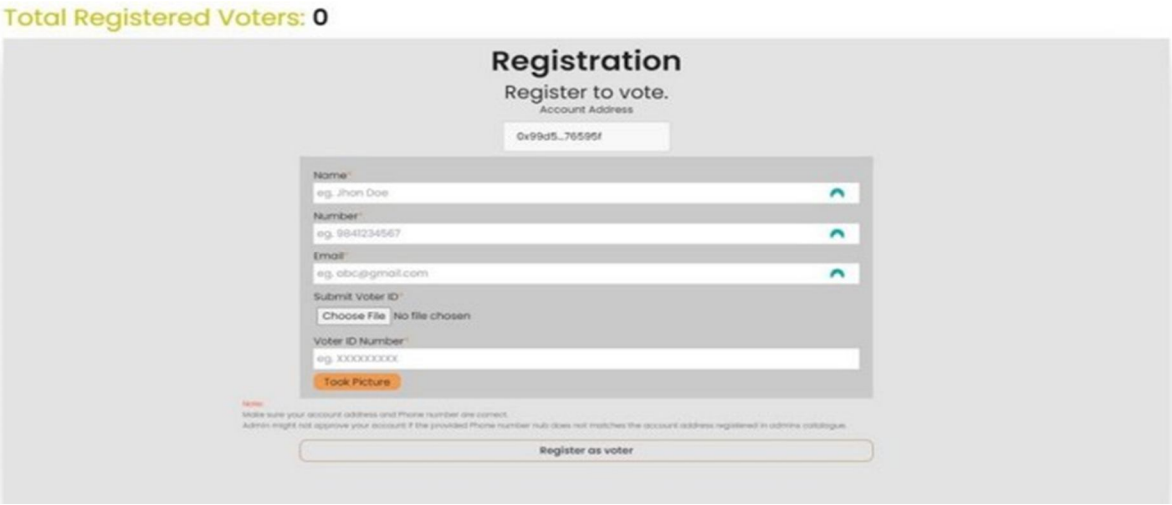


Fig. 5 Voter page for registration

```
// Pseudo-code for an E-Voting DApp with Homomorphic Encryption

// Contract state variables
contract Election {
    struct Voter {
        bool hasVoted;
        bytes32 encryptedVote; // Encrypted vote
    }

    struct Candidate {
        string name;
        uint voteCount;
    }

    mapping(address => Voter) public voters;
    Candidate[] public candidates;

    // Public key for Paillier homomorphic encryption
    struct PublicKey {
        uint n; // modulus
        uint g; // generator
    }

    PublicKey public publicKey;

    // Election organizer sets the public key
    function setPublicKey(uint _n, uint _g) public {
        require(msg.sender == organizer, "Only the organizer can set the public key");
        publicKey = PublicKey(_n, _g);
    }

    // Function for a voter to cast their encrypted vote
    function vote(uint _candidateIndex, uint _ciphertext) public {
        require(!voters[msg.sender].hasVoted, "You have already voted");
        require(_candidateIndex < candidates.length, "Invalid candidate index");

        // Encrypt the candidate index using Paillier homomorphic encryption
        uint encryptedVote = paillierEncrypt(_ciphertext);
```

Fig. 6 First Pseudo Code for application

```
        // Record the encrypted vote
        voters[msg.sender].encryptedVote = bytes32(encryptedVote);
        voters[msg.sender].hasVoted = true;

        // Increment the candidate's vote count
        candidates[_candidateIndex].voteCount++;
    }

    // Function to decrypt and count the votes
    function countVotes() public view returns (uint[]) {
        uint[] memory decryptedVoteCounts = new uint[](candidates.length);

        for (uint i = 0; i < candidates.length; i++) {
            for (address voterAddress : voters) {
                Voter storage voter = voters[voterAddress];
                if (voter.hasVoted) {
                    uint decryptedVote = paillierDecrypt(uint(voter.encryptedVote));
                    if (decryptedVote == i) {
                        decryptedVoteCounts[i]++;
                    }
                }
            }
        }

        return decryptedVoteCounts;
    }

    // Paillier encryption algorithm (simplified)
    function paillierEncrypt(uint plaintext) internal view returns (uint) {
        // Replace with the actual Paillier encryption algorithm
        return (plaintext ** publicKey.n) % (publicKey.n ** 2);
    }

    // Paillier decryption algorithm (simplified)
    function paillierDecrypt(uint ciphertext) internal view returns (uint) {
        // Replace with the actual Paillier decryption algorithm
        uint lambda = (publicKey.n - 1) * (publicKey.n - 1);
        return ((ciphertext ** lambda) - 1) / publicKey.n;
    }
}
```

Fig. 7 Second Pseudo Code for application

IV. CONCLUSION

A. *Conclusion*

Trustworthy voting is a cornerstone of democracy, requiring public confidence in the electoral process. Traditional paper- based elections often lack credibility and need modernization. Digital voting technologies can make elections more affordable, efficient, and accessible in contemporary culture. These technologies normalize voting, reduce the gap between voters and officials, and encourage democratic engagement. The project's goal is to establish a blockchain-based electronic voting system using smart contracts for secure, cost-effective, and private elections. Future plans include developing specialized voting client designs for roles like election commissions and party-affiliated candidates. Overall, the project seeks to enhance democracy by improving the transparency and efficiency of the voting process.

B. *Discussion and Future work*

In the future, efforts will be made to explore the integration of the Paillier cryptosystem as a Solidity library. This change has the potential to streamline the verification of each vote within the current system.

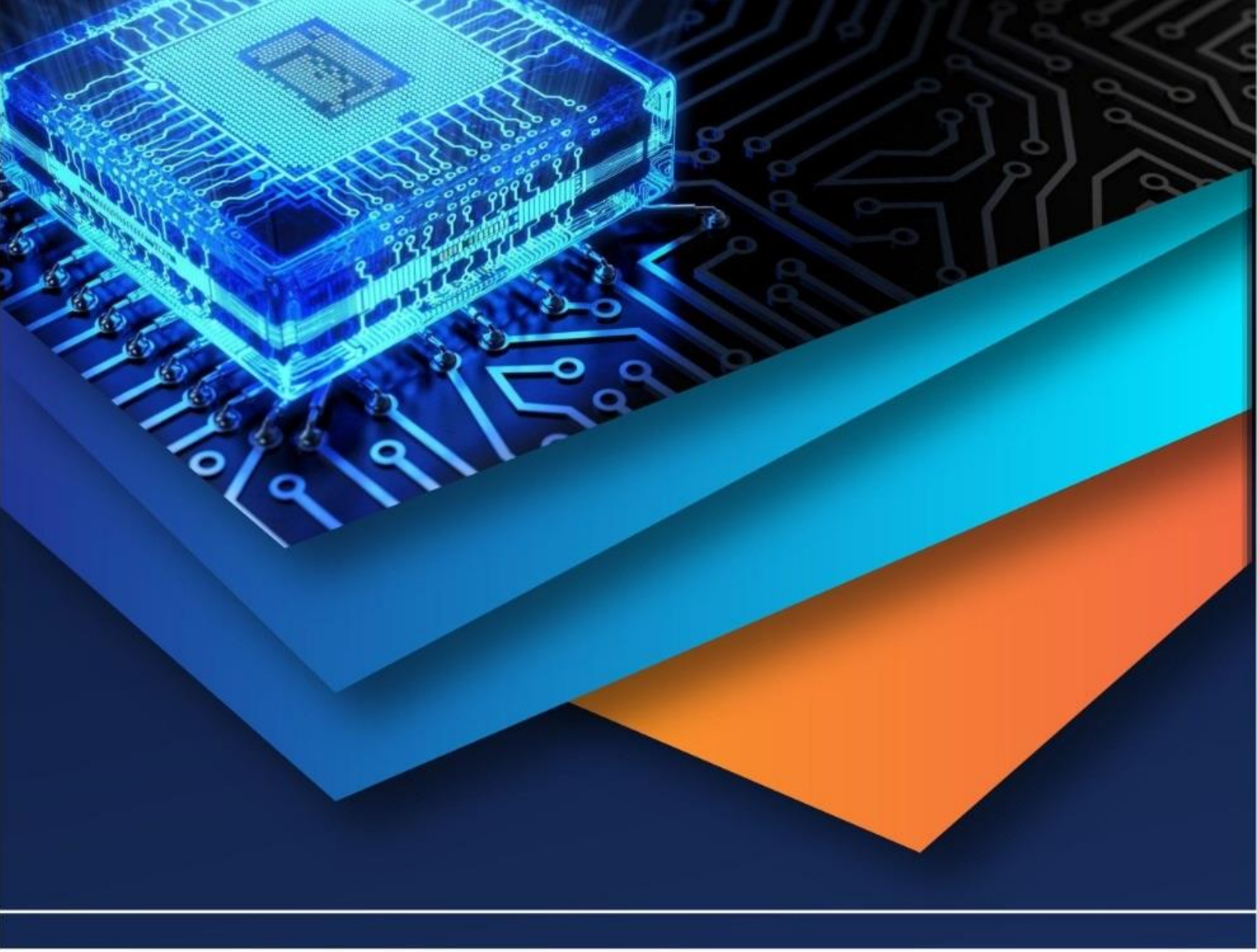
Additionally, incorporating the Paillier library into Solidity would simplify the process of generating new private and public keys for each ballot. This step is crucial in developing a transparent e-voting system with end-to-end verifiability.

To establish trust in e-voting systems, we are enhancing existing blockchain-based infrastructure with an additional layer dedicated to ensuring provenance. This added layer is integral to our goal of building a trustworthy e-voting solution.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] Ehiagwina, F. O., Iromini, N. A., Olatinwo, I. S., Raheem, K., Mustapha, K. (2022). A State-of-the-Art Survey of Peer- to-Peer networks: research directions, applications and challenges. Journal of Engineering Research and Sciences, 1(1), 19–38. https://doi.org/10.55708/js0101003
[2] Song, J., Moon, S. J., Jang, J. (2021). A Scalable Implementation of Anonymous Voting over Ethereum Blockchain.
[3] Sensors, 21(12), 3958. https://doi.org/10.3390/s21123958
[4] Alaya, B., Laouamer, L., Msilini, N. (2020). Homomorphic encryption systems statement: Trends and challenges. Com- puter Science Review, 36, 100235. https://doi.org/10.1016/j.cosrev.2020.100235
[5] Imperial, M. (2021). The Democracy To Come? An enquiry into the vision of Blockchain-Powered E-Voting Start-Ups.
[6] Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.587148
[7] Wang, Q., Chen, S., Xiang, Y. (2021). Anonymous blockchain-based system for consortium. ACM Transactions on Man- agement Information Systems, 12(3), 1–25. https://doi.org/10.1145/3459087
[8] Gao, S., Zheng, D., Guo, R., Jing, C., Hu, C. (2019). An Anti-Quantum E-Voting protocol in blockchain with audit function.
[9] IEEE Access, 7, 115304–115316. https://doi.org/10.1109/access.2019.2935895
[10] Shahzad, B., Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7, 24477–24488. https://doi.org/10.1109/access.2019.2895670
[11] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., Guizani, N. (2020b). Securing Smart Cities through Blockchain Technol- ogy: Architecture, Requirements, and Challenges. IEEE Network, 34(1), 8–14. https://doi.org/10.1109/mnet.001.1900178
[12] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., Guizani, N. (2020). Securing Smart Cities through Blockchain Technol- ogy: Architecture, Requirements, and Challenges. IEEE Network, 34(1), 8–14. https://doi.org/10.1109/mnet.001.1900178
[13] Mohanta, B. K., Jena, D., Panda, S. S., Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things, 8, 100107. https://doi.org/10.1016/j.iot.2019.100107
[14] Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems, 102, 902–911. https://doi.org/10.1016/j.future.2019.09.028
[15] Çabuk, U. C., Adıgüzel, E., Karaarslan, E. (2018). A survey on Feasibility and Suitability of blockchain Techniques for the E-Voting Systems. Nternational Journal of Advanced Research in Computer and Communication Engineering, 7(3), 124–134. https://doi.org/10.17148/ijarcce.2018.7324
[16] Wongthongtham, P., Marrable, D., Abu-Salih, B., Liu, X., Morrison, G. M. (2021). Blockchain-enabled Peer-to-Peer energy trading. Computers Electrical Engineering, 94, 107299. https://doi.org/10.1016/j.compeleceng.2021.107299
[17] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019
[18] Ahmed, M. T. A., Hashim, F., Hashim, S. J., Abdullah, A. (2023). Authentication-Chains: Blockchain-Inspired lightweight authentication protocol for IoT networks. Electronics, 12(4), 867. https://doi.org/10.3390/electronics12040867
[19] Abuidris, Y., Kumar, R., Yang, T., Onginjo, J. O. (2020). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. Etri Journal, 43(2), 357–370. https://doi.org/10.4218/etrij.2019- 0362
[20] González, C. D., Mena, D. F., Muñoz, A. M., Rojas, O., Sosa-Gómez, G. (2022). Electronic voting system using an enterprise blockchain. Applied Sciences, 12(2), 531. https://doi.org/10.3390/app12020531
[21] Pawlak, M., Poniszewska-Maran´da, A. (2021). Trends in blockchain-based electronic voting systems. Information Pro- cessing and Management, 58(4), 102595. https://doi.org/10.1016/j.ipm.2021.102595
[22] Jafar, U., Aziz, M. J. A., Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and open Research Chal- lenges. Sensors, 21(17), 5874. https://doi.org/10.3390/s21175874
[23] Farooqui, Y. .; Parikh, S. M. . Secure and Transparent Supply Chain Management Using Blockchain and IoT. IJRITCC 2023,11,01-12.
[24] Yassir Farooqui, et al. An Effective Supply Chain Model Using Blockchain in IoT With Trust Enabled Hybrid Concensus Algorithm. IJRITCC 2023,11,229-240.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)