iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50618

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 11 Issue IV Apr 2023- Available at www.ijraset.com

E -Voting System using Blockchain

Namrata Jaiswar[1], Soham Deodhar[2], Harish Gupta[3], Prof. Dnyaneshwar Kapse[4]
[1, 2, 3]*B.E. Computer Science, Rajiv Gandhi Institute of Technology, Mumbai University, Maharashtra, India*
[4]*Professor, Dept. of Computer Science Engineering, Rajiv Gandhi Institute of Technology, Mumbai University, Maharashtra, India*

Abstract: Designing a voting system that ensures fairness, privacy, and security is a significant challenge. The lack of trust in election systems among large sections of society worldwide is a major concern for democracy. Flawed voting systems pose a threat to democracies, including governing bodies, co-operating societies, and student councils. Vote rigging, hacking of electronic voting machines (EVMs), election manipulation, and booth capturing are the key issues with the current electoral system. To address these issues, we propose using novel technologies such as blockchain and Merkel trees, which are well-known for their security benefits. Our system builds on popular blockchain frameworks that provide blockchain as a service, while preserving participants' anonymity and enabling public scrutiny. Blockchain is a unique technology of our time that promises to enhance the resilience of digital voting platforms. It presents an opportunity to leverage the benefits of blockchain, such as cryptographic foundations and transparency, to achieve an efficient digital voting system.
Keywords: Blockchain, e-voting, electronic voting, internet voting.

I. INTRODUCTION

The block-based digital voting system is a solution that has been designed to address several security risks related to electronic voting machines and online voting platforms. This system employs a closed, private Peer-to-Peer (P2P) network and is capable of functioning in a decentralized manner. The primary objective of this voting system is to provide a fair and secure election process for organizations. Users will be able to register as voters and cast their votes after completing the necessary security and login procedures. The administrator will oversee the maintenance of the blockchain during downtimes, live hot fixing, creating backups, and managing the voter list. The administrator will also be capable of customizing the voting portal's Graphical User Interface (GUI) as per the organization's requirements. The entire voting system will consist of a limited number of terminals (such as laptops), typically 3-5, joined in a P2P network, built using the Ethereum framework. During the voting process, users may cast their votes using these terminals, and a copy of the vote blockchain will be stored locally on each terminal. Administrators may use these terminals to add or delete voters to the voter registration list. At the end of the voting period, the administrators may disclose the election results. The system's design ensures that the entire process is transparent and tamper-proof, with the blockchain serving as an immutable record of all votes. Additionally, the system's decentralized nature eliminates the risk of a single point of failure or cyber-attack, thus enhancing the overall security of the voting process In summary, the block-based digital voting system offers a secure and transparent method for organizations to conduct fair and reliable elections. Its decentralized design, coupled with the use of blockchain technology, ensures that the system is tamper-proof and immune to cyber-attacks.

II. LITERATURE SURVEY

III. EXISTING SYSTEM

[5] The simple rationalization could be a ‘chain’ of blocks. A block is associate degree mass set of information. know-edge square measure collected and method 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.

[6] Elections for Secretary and other members in Colleges or Organizations are often challenging due to candidates being from different departments, which makes coordinating votes difficult. To address this issue, a web-based polling system has been developed that enables candidates to vote confidentially from any department, using Visual Cryptography to ensure security. The College E-Voting System Using Visual Cryptography (VC) is designed to provide a secure platform for casting votes for critical and confidential internal college decisions. The system allows voters to cast their vote remotely and ensures full confidentiality by applying appropriate security measures. A unique password is generated by merging the two shares (Black & White dotted Images) using VC scheme, and only authorized voters can log into the system to cast their vote.

©IJRASET: All Rights are Reserved

[7] The E-voting system is based on the Prêt à Voter approach and aims to provide a secure digital voting experience that does not compromise usability. The system considers specific requirements such as privacy, eligibility, convenience, receipt-freeness, and verifiability.

It uses a web-based interface with finger printing to protect against double voting and has a user-friendly administrator interface to manage voters, constituencies, and candidates. The system ensures all voters have equal rights of participation, develops a fair and healthy competition among candidates, and keeps the anonymity of voters preserved. The cryptographic hash of the transaction (ID) is emailed to the voter as proof of their vote, which can later be tracked outside the constituency.

IV. DRAWBACKS

[5] The current e-voting system does not support local languages, which are essential for voters in suburban and rural areas. Additionally, the system lacks an authentication process for users and verification of Aadhar cards, both of which are crucial steps in ensuring the integrity of the voting process. As e-voting is a critical part of our democratic process, it is imperative that the security of the system is a top priority.

[6] The drawback of this proposed e-voting system is that it assumes all nodes are trustworthy and operate with good intentions. However, there is a risk that some nodes may be compromised or manipulated, leading to inaccuracies or manipulations in the voting results.

Additionally, the reliance on private and public keys can also be a weakness, as these keys can be stolen or hacked. Another potential issue is the lack of anonymity in the voting process, as each node's public key is shared with all other nodes, making it possible to trace the vote back to a specific individual or group. Finally, the system does not address the issue of voter coercion or influence, which can still occur in the electronic voting process.

[7] The electronic voting, including the proposed blockchain-based approach, is the potential for cybersecurity risks. Hackers or other malicious actors could attempt to manipulate or compromise the system, potentially altering or even invalidating the results. Additionally, there are concerns about the privacy and anonymity of voters, as well as the potential for technical glitches or errors that could affect the accuracy and fairness of the election. The cost of implementing and maintaining such a system may be prohibitively expensive for some organizations or governments, which could limit its accessibility and potential impact.

V. PROPOSED SYSTEM

Blockchain technology is widely used for recording and maintaining a tamper-proof database. In the context of e-voting systems, permissioned blockchain is used, which differs from the independently random nodes used in Bitcoin. Before the election process starts, each node generates a private key and a public key, and shares the public key with all the nodes in the election process. This ensures that each node has a list of public keys of all the nodes involved in the process.

During the election, each node collects the votes from the voters and validates the incoming blocks to ensure their authenticity. Once a valid block is received, the database is updated with the data in the block.

After the database is updated, the node checks whether it has the turn to submit the next block. If it does, the node creates and submits a block that includes its node ID, the next node ID to be used as the token, a timestamp, the voting results, the hash of the previous node, and the digital signature of the node.

This method aims to maintain the integrity of the election data and prevent any tampering or manipulation of the process. By using a permissioned blockchain, only authorized nodes can participate in the election process, and all actions are recorded and stored in a secure and immutable database. This ensures that the election process is transparent and trustworthy.

VI. SYSTEM ARCHITECTURE

An e-voting system is a digital platform that enables citizens to cast their vote in an election or referendum using the internet or other electronic means.

However, traditional e-voting systems have been subject to security concerns, and blockchain technology provides a secure and transparent platform for implementing e-voting systems. Here is an overview of the system architecture for an e-voting system using blockchain technology an e-voting system using blockchain technology provides a secure, transparent, and tamper-proof platform for conducting elections. The system architecture includes a user interface, smart contracts, blockchain network, security features, and results verification.

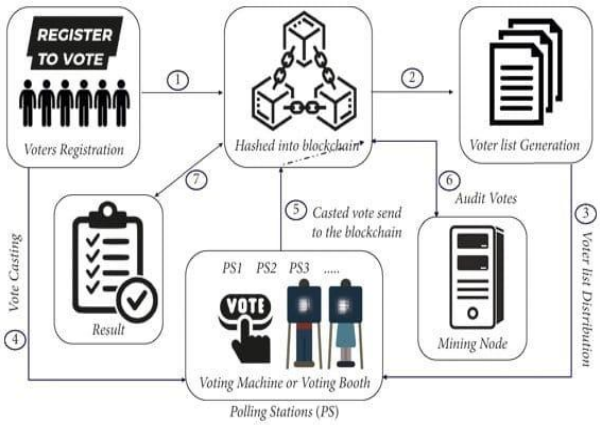
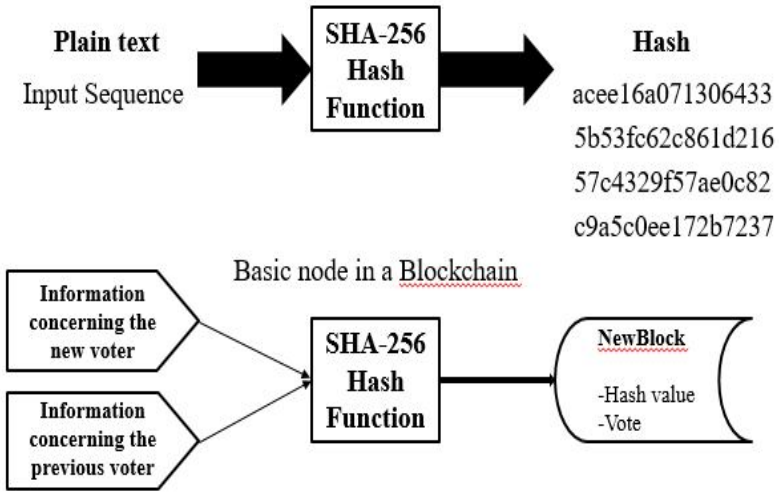


Fig: 1.1 System architecture

1) *User Interface:* The user interface is the front-end of the e-voting system that provides a user-friendly interface for voters to cast their votes. It includes web and mobile applications that enable voters to login, view candidate lists, and cast their vote.
2) *Smart Contracts:* Smart contracts are self-executing programs that are deployed on a blockchain network to automate the execution of transactions. In an e-voting system, smart contracts manage the voting process, store the candidate lists, and record the votes. The smart contract also ensures that only authorized voters can cast their vote and prevents double voting.
3) *Blockchain Network:* The blockchain network is a decentralized and distributed database that stores the transaction data in blocks. It provides a secure and tamper-proof platform for recording the votes and verifying the authenticity of the votes. The blockchain network used for an e-voting system should be public, transparent, and accessible to all the stakeholders.
4) *Security:* Security is a critical component of an e-voting system, and blockchain technology provides several security features such as immutability, transparency, and cryptography. Additionally, multi-factor authentication, encryption, and digital signatures can be used to enhance the security of the e-voting system.
5) *Results Verification:* After the voting process is complete, the results of the election can be verified using the blockchain network. The blockchain network enables all the stakeholders to verify the election results, ensuring the integrity of the process

VII. ALGORITHM

A. *SHA-256 Algorithm*



The SHA-256 algorithm is a cryptographic hash function that takes an input message of any length and produces a fixed-size output (256 bits). Here are the steps involved in the SHA-256 algorithm

Steps

1) Padding: If the length of the input message is not a multiple of 512 bits, padding is added to the message to make its length a multiple of 512 bits. The padding consists of a single "1" bit, followed by enough "0" bits to make the length of the message a multiple of 512 bits, and finally the length of the original message is appended as a 64-bit big-endian integer.
2) Initializing hash values: The algorithm uses eight 32-bit words (also known as "hash values") as the initial state. These words are derived from the first 32 bits of the fractional parts of the square roots of the first 8 prime numbers.
3) Breaking the message into 512-bit chunks: The padded message is broken up into 512-bit chunks, and each chunk is processed in turn.
4) Message schedule: A "message schedule" is derived from each chunk of the message. This involves creating 64 additional 32-bit words, based on the previous 16 words and some bitwise operations.
5) Compression function: The message schedule and hash values are then used in a "compression function" that operates on 64 32-bit words at a time. The compression function uses a series of logical and arithmetic operations to transform the hash values.
6) Final hash value: After all chunks of the message have been processed, the resulting hash value is the concatenation of the final hash values for each chunk.
7) The SHA-256 algorithm is designed to be secure against collision attacks, where two different inputs produce the same hash output, as well as pre-image attacks, where an attacker tries to find an input that produces a specific hash output.

B. Proof of work

Proof of Work (PoW) is a consensus algorithm used in blockchain networks to validate transactions and create new blocks. Here are the steps involved in the PoW algorithm:

Steps

1) Transaction validation: Before miners can start creating a new block, they must validate the transactions in the pool to ensure they are valid and meet the network's rules.
2) Block header creation: Once the transactions have been validated, the miner creates a block header that includes the previous block's hash, the current timestamp, the transactions included in the block, and a nonce (a random number).
3) Hashing: The miner then takes the block header and hashes it using the SHA-256 algorithm, producing a 256-bit hash value.
4) Target threshold comparison: The miner then compares the hash value to the target threshold set by the network. The target threshold is a number that determines the difficulty of the PoW puzzle. It is adjusted regularly to maintain a consistent block.

Difficulty adjustment: If the hash value is lower than the target threshold, the miner has successfully solved the PoW puzzle and can broadcast the block to the network. If the hash value is higher than the target threshold, the miner adjusts the nonce and repeats the hashing process until a suitable hash value is found. Reward distribution: Once a miner successfully creates a new block, they are rewarded with newly minted cryptocurrency and transaction fees.

C. The RSA (Rivest–Shamir–Adleman)

The RSA (Rivest–Shamir–Adleman) algorithm is a widely used asymmetric cryptographic algorithm for secure communication. Here are the steps involved in the RSA algorithm.

Steps

1) Key generation: A pair of public and private keys is generated by selecting two large prime numbers, p and q. The product of p and q is called the modulus, n. The private key consists of the two primes, p and q, while the public key consists of the modulus, n, and an exponent, e, which is usually a small prime number.
2) Encryption: To encrypt a message, the sender uses the recipient's public key to transform the message into ciphertext. The message is first converted into a numerical representation, and then raised to the power of the exponent, e, modulo the modulus, n.
3) Decryption: To decrypt the ciphertext, the recipient uses their private key to transform the ciphertext back into the original message. The ciphertext is raised to the power of the private exponent, d, modulo the modulus, n.
4) Digital signatures: RSA can also be used for digital signatures to ensure the authenticity and integrity of messages. To sign a message, the sender computes a hash of the message, raises it to the power of the private key exponent, and then takes the modulus of the result with the modulus, n. The resulting value is the digital signature.
5) Key management: RSA keys should be kept confidential and secure to prevent unauthorized access. Public keys can be distributed widely, while private keys should be protected and kept secret.

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

VIII. METHODOLOGY

An e-voting system using blockchain technology can ensure the integrity and transparency of the voting process. The methodology involves creating a blockchain network that consists of a decentralized ledger where each block contains a record of all votes cast. The voting process would begin with voters registering their identities on the blockchain network, which would be verified by multiple nodes in the network. When a voter casts their vote, it would be recorded on the voting results would be calculated by counting the number of votes for each candidate based on the hashes stored on the blockchain. The decentralized nature of the blockchain network ensures that the voting results cannot be altered, and the transparency of the system allows for audits and verification by any interested party.

To prevent double voting or voter fraud, the blockchain network can implement smart contracts that restrict a voter from casting multiple votes or verifying that the identity of the voter is genuine.

1) *Phase 1: Requirements gathering:* Define the requirements of the e-voting system, including the type of election, the number of voters, the level of security required, and the expected performance.
2) *Phase 2: Design:* Based on the requirements, design the architecture of the e-voting system, including the blockchain structure, the consensus mechanism, the smart contracts, and the user interface.
3) *Phase 3: Development:* Development: Develop the e-voting system using blockchain technology, including the smart contracts for managing the voting process, the user interface for voters, and the administrative interface for managing the election.
4) *Phase 4: Testing & Deployment:* Test the e-voting system to ensure that it meets the requirements and that there are no vulnerabilities that could compromise the security of the system. Deploy the e-voting system on the blockchain network, making it available for voters to use.
5) *Phase 5: Voter Registration:* Voter registration: Implement a voter registration process, where voters are authenticated using their unique identification credentials. This could involve a two-factor authentication process, where the voter is required to provide a password and a biometric identifier.
6) *Phase 6: Voting Process:* Voting process: Implement a secure voting process, where voters can cast their votes using the e-voting system. The blockchain should ensure that each vote is recorded accurately and that no votes are duplicated or modified.
7) *Phase 7: Vote Counting:* Develop a vote counting mechanism, where the votes are tallied and the results are announced. The blockchain should ensure that the results are transparent and cannot be altered.
8) *Phase 8: Post-election Audit:* Post-election audit: Conduct a post-election audit to ensure that the voting process was fair and transparent. The blockchain should enable auditors to verify that the votes were recorded and counted accurately.

IX. FUTURE ASPECTS

The use of blockchain technology in e-voting systems has the potential to revolutionize the way we conduct elections, making them more secure, transparent, and accessible. Here are some future aspects of e-voting systems using blockchain:

Increased Security: Blockchain technology provides a decentralized and tamper-proof platform for e-voting. It ensures that the votes are recorded and counted accurately and cannot be altered or manipulated. In the future, e-voting systems using blockchain will likely become more secure using advanced cryptographic techniques and multi-factor authentication.

Improved Transparency: The use of blockchain in e-voting systems will enhance the transparency and auditability of the electoral process. Every vote cast will be recorded on the blockchain, and the entire transaction history will be available for scrutiny by anyone. This will help build trust in the electoral process and prevent any attempts to manipulate the results.

Greater Accessibility: E-voting systems using blockchain will increase accessibility for voters who are unable to physically attend polling stations. Voters can cast their vote from anywhere using a mobile device or computer. This will increase voter turnout and make the electoral process more inclusive.

X. CONCLUSIONS

In conclusion, the use of block chain technology for e-voting systems provides several technical advantages, such as tamper-proof and transparent record-keeping, decentralized consensus mechanisms, and increased security through cryptographic protocols. By utilizing a distributed ledger, the block chain can ensure that votes are immutable, auditable, and anonymous, providing a more secure and trustworthy voting system. However, there are still technical challenges that must be addressed, such as scalability, interoperability, and user accessibility. Overall, the use of block chain technology has the potential to revolutionize the e-voting landscape, but careful consideration and further development are necessary to ensure its effectiveness and practicality in real-world scenarios.

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

REFERENCES

[1] Emanuele Bellini, Paolo Ceravolo and Ernesto Damiani, "Blockchain-based E-Vote as a service", IEEE 12th International Conference on Cloud Computing, 2019. Available from https://ieeexplore.ieee.org/document/8814575

[2] Julija Golosova; Andrejs Romanovs, "The Advantages and Disadvantages of the Blokchain Technology, IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering, 2018. Available from https://ieeexplore.ieee.org/document/8592253

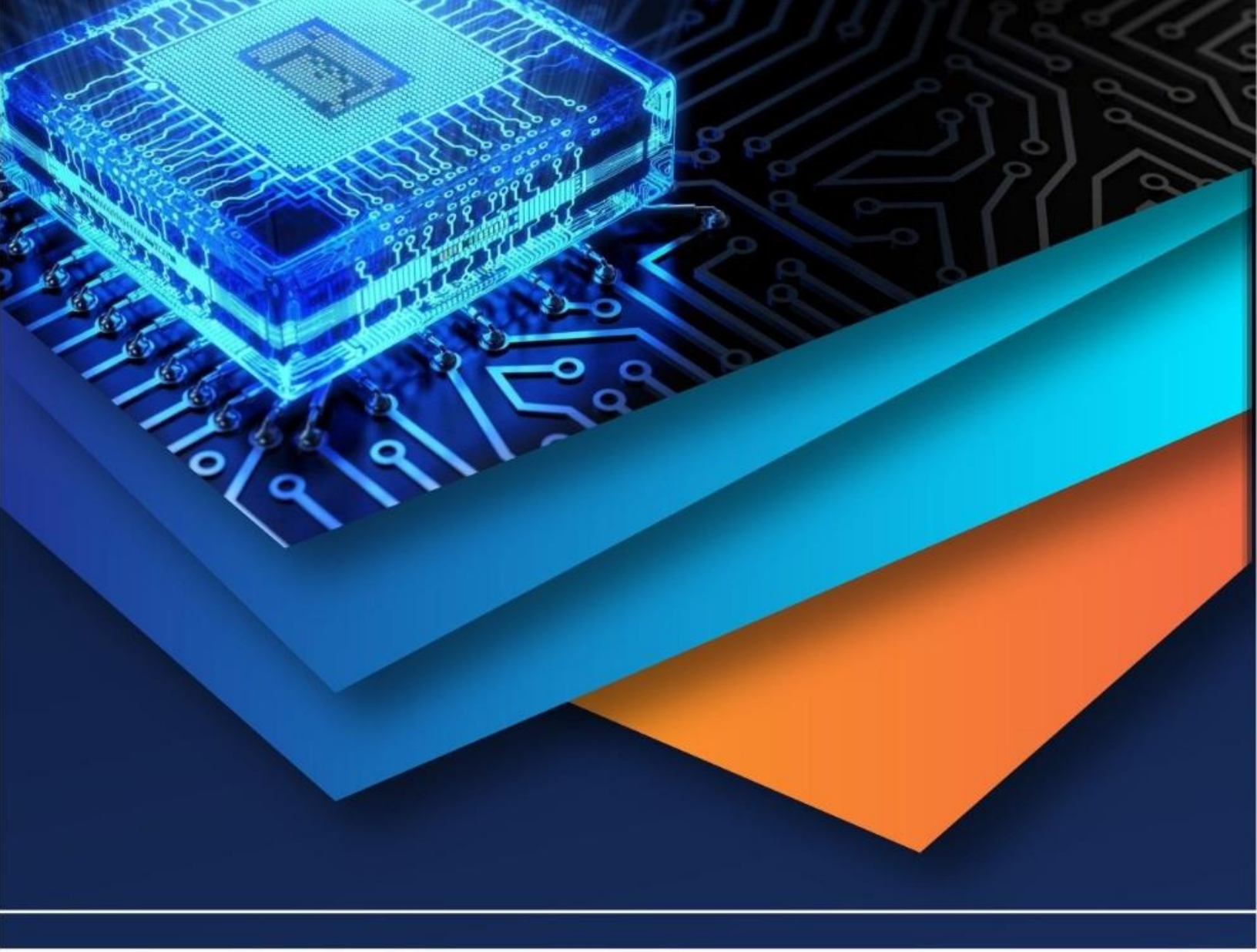
[3] Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data, 2017. Available website https://ieeexplore.ieee.org/document/8029379

[4] Dipali Pawar, Pooja Sarode, Shilpa Santpure, Poonam Thore, "Implementation of Secure Voting System using Blockchain", International Journal of Engineering Research & Technology (IJERT), 2020. Available from https://www.ijert.org/research/implementation-of-secure-voting-system-using-blockchain-IJERTV9IS060974.pdf.

[5] Prof.AnitaA. Lahane, ∗, JunaidPatel, TalifPathan, andPrathmeshPotdar1, "Blockchain technology based- voting system.", ICACC- 2020 ITM Web of Conferences **32**, 2020. Available from https://doi.org/10.1051/itmconf/20203203001

[6] Prof. Pallavi Shejwal1, Aditya Gaikwad2, Mayur Jadhav3, Nikhil Nanaware 4, Noormohammed Shikalgar5 E-voting using blockchain technology, 2018 IJRAR December 2018, Volume 5, Issue 04. www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138).

[7] Kashif Mehboob Khan1, Junaid Arshad2, Muhammad Mubashir Khan1 1 NED University of Engineering and Technology, Pakistan 2 University of West London, UK.https://core.ac.uk/display/155779036?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1



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)