iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.48548

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 III Mar 2023- Available at www.ijraset.com

SoulBound E-Voting System

Aayush Sagar[1], Dr. Sudha Narang[2], Ayush Seth[3], Siddhant Jain[4]
[1]*Maharaja Agrasen Institute of Technology, New Delhi, India*
[2]*(Asst. Prof., CSE), Department of Computer Science and Engineering*
[3, 4]*Maharaja Agrasen Institute of Technology, New Delhi, India*

Abstract: ***The right to vote is a fundamental right of citizens of democratic countries around the world. This is necessary so that citizens have a say in the choice of who represents them or in matters affecting them. The aspects of security and transparency are still threats from widespread elections with traditional systems. For years, democracies around the world have moved from sticking to paper ballots to electronic voting machines. These machines are not tamper-proof despite system checks, security procedures and election protocols. However, hacking and tampering with these machines is becoming more frequent as the number and methods of attackers increase. Physical access to the EVM, even for a few minutes, is enough to crack it. To ensure a fair and reliable election process, safety and security must be ensured throughout the process. A single organization still exists to administer the centralized system used for general elections. When organizations have complete control over their databases and systems, they can disrupt the database of important opportunities, which can cause a lot of problems in traditional election systems. Because networked software devices are vulnerable, the proposed work applies security concepts based on popular blockchain technology. It is currently being implemented with the goal of securing online money transactions in the digital economy. Blockchain has paved the way for cryptocurrencies such as Bitcoin and Ethereum. A blockchain is a distributed and non-translatable ledger in which data is added and updated in real time based on the consensus of nodes running software on the network. However, once data is added to the registry, you cannot delete or edit the data from the database. Therefore, counterfeit voting is impossible, increasing the reliability of the electronic voting system. As a result, governments around the world are exploring blockchain as a means to make general elections tamper-proof and transparent, with the goal of enabling a system where everyone trusts data and is tamper-proof. Using blockchain for database distribution of electronic voting systems can reduce one of the sources of fraud in database manipulation.***

Keywords: e-voting, SBT, blockchain, BABT

I. INTRODUCTION

Electronic voting is widespread in social life. However, it is not clear how to ensure that the outcome will be honored if the decision has a financial or political context. Accuracy, security and privacy are always the most important characters. Secure electronic voting is a type of secure multi-party computation. In voting, many people make decisions, and the decisions they make may be kept secret.

Most electronic voting systems require a reliable public bulletin board to provide a consistent view to all voters. However, it is up to the election administrator to prove that a public bulletin board can be completely reliable. Some people realize that blockchain can be used as a message board because the content is publicly approved.

The blockchain is served as a decentralized database that provides new tools for creating a decentralized and trustless system. In the blockchain system, there is no centralized trusted coordinator. Instead, each node participating in the blockchain system holds the block of data locally. The blockchain is maintained by a decentralized and open peer-to-peer network. Initially, the technology was designed to transfer money. With its development, researchers are trying to reuse Blockchain in other areas of research such as coordinating the Internet of Things, carbon dating, and healthcare. This triggered the invention of Ethereum, known as a milestone in blockchain development. It has a full Turing programming language and users can realize this functionality by smart contracts in the Ethereum network.

The blockchain can be used as a trusted public bulletin board for the voting system. In addition, the smart contract on the blockchain acts as a trusted computer whose results are publicly trusted. However, just replacing the bulletin board with blockchain is not a good idea. Because there will be too many transactions for voters to distinguish and the computation on the blockchain is very difficult, that can be seen.

In addition, the smart contract on the blockchain acts as a trusted computer whose results are publicly trusted. To ensure the anonymity of the users SoulBound NFT is used.

II. LITERATURE SURVEY

There are some noteworthy works already done in this field which are cited to get the general idea needed for this study and to understand some key concepts. We referred to a research paper titled “E-Voting Using Blockchain Technology” by Sai Charan, Pentapati, and Prema to get an overview of how they attempted to solve a similar problem using Ethereum as a blockchain network.
A research paper entitled “E-Voting Using Blockchain Technology” by Shejwal, Gaikwad, Jadhav and Nanawar was also mentioned to better understand how Ethereum works and whether it can be included in the study. Also, the advantages and disadvantages of using public key and merkle tree to complete the election process were understood. A Merkle tree is a type of tree that contains leaf nodes labeled with data block hashes and non-leaf nodes labeled with the cryptographic hashes of child nodes.
There are various voter authentication strategies. According to Kriti Patidar and Dr Jain voter authentication can be done using cryptography with a private key that must be provided to voters before an election begins. A voter must be registered by a specific agency, and a voter key must be generated and delivered to the voter during registration.
The paper written by E. Glen Weyl, Puja Ohlhaver and Vitalik Buterin explained the concept of Soul Bound Token. These are Non-Fungible Tokens which are nontransferable and are unique for each and every wallet holder. It is minted when then user completes KYC with the organization. These are publicly visible as it is validated as proof of concept. SBT will help us in tracing the social provenance. It can also represent the information of an individual in the virtual world.
Understanding of various topics such as blockchain security, blockchain structure, various existing blockchain networks, general strengths and weaknesses of voting systems, and many other topics after referring to various related works was obtained. Various consensus algorithms such as Proof of Work and Proof of Existence were also introduced. This review helped us formulate our own research.

III. METHODLOGY

Blockchain is a new technology that guarantees data immutability using cryptographic functions, consensus algorithms, and protocols while providing network decentralization with no single point of failure. Blockchain is a public, decentralized ledger technology, a database with copies of it spread across several nodes concurrently.
Blockchain does not have a central authority whose functions include keeping track of and managing the transactional ledger. The version of the ledger's validity is determined by a way for validating nodes to agree about something. The secure validation of data using blockchain technology data consistency of a transaction. For instance, Bitcoin is the first by Satoshi Nakamoto, a blockchain-based application.
A decentralized peer-to-peer network with open membership manages the blockchain. This technology is initially intended for money transfers. Researchers are attempting to leverage Blockchain as it develops in other study areas such managing the Internet of Things, carbon dating, and healthcare. This led to the creation of Ethereum, which is widely seen as a turning point in the evolution of blockchain. It has a Turing-complete programming language, and users can use the Ethereum network's smart contracts to accomplish its function. Blockchain has the potential to serve as the secure public message board for the voting system. Additionally, the blockchain's smart contract functioned as a trusted computer whose output was accepted by everyone. However, it is not a smart idea to just replace the bulletin board with blockchain. Voters won't be able to distinguish between enough transactions, and the blockchain's computation is quite difficult.
The main objective of the web application is to act as Application Programming Interface to cast vote and create new polls.
The scope of the system is very broad, as it can be used in any organization where elections play a major role in electing their representatives The system can be adapted to meet the needs and needs of the number of participants using the system's strong encryption techniques.

A. Types of Blockchains

1) Public Blockchain

These are unrestricted blockchains. Anyone with an internet connection can access the network and begin sending transactions and validating blocks. Such networks typically provide some type of reward to users who validate the blocks.
In any case, the consensus techniques used by this network to validate transactions often involve Proof of Work or Proof of Stake. In the truest sense, it is a "Public" network. You don't need anyone's permission to download the protocol while using a public blockchain architecture. The ideal paradigm that makes the technology sector so lucrative is represented by the public blockchains.
As a result, the ecosystem is entirely decentralized and not under the authority of any one entity.

2) Private Blockchain

Only through an invitation that authenticates and verifies the participant's identity or other necessary information can they join a priv ate blockchain network.

The validation is carried out either by the network operator(s) or by the network itself, using smart contracts or other automated appr oval techniques, to carry out a well-defined set protocol.

Private blockchains have restrictions on who can use the network. The network's private nature can limit which users can run the cons ensus process that determines the mining rights and rewards if it has mining capabilities. The shared ledger might also be maintained by a small group of users.

3) Hybrid Blockchain

A hybrid blockchain is frequently described as a fusion of both public and private blockchain. It combines key elements of both public and private blockchains, and by combining the greatest features of both, it creates transactions and data that are private. However, they can still be confirmed as essential, for instance by allowing access through a smart contract. Private information is preserved within the network but is still verifiable. The transactions cannot be changed on a private entity's hybrid blockchain. Companies can build their own permission-based networks in addition to publicly accessible ones thanks to hybrid blockchains. Anyone who participates in such hybrid blockchains has full network access. The core structure of blockchain is decentralization, transparency, consistency, independence, open source, anonymity, and consistency.

a) Blockchain as a data structure: A blockchain contains a list of features and sets them up as blocks. A project starts with one block, called the first block. More blocks have been added as part of increasing the exchange volume. The previous block is linked to the current block. Blockchain provides this type of information structure. Blockchains are usually designed with care and simplicity.

b) Decentralized: Shared Organization; A collection of frameworks is one of the key features of fragmented and amazing blockchain development. Anyone can save applications and then access them over the Internet without outside assistance. Store all your exchanges, including securities, records, contracts, computer assets, and access them in the future with your private key.

c) Consistency: Consistency is how the blockchain structure allows and trusts transactions before they are added to the chain. The exchange will be considered void if the work violates any of the agreed conditions. The blockchain is passed to the show on a show-by-show basis, which may be some authority or approval. Community contracts stipulate that anyone can jointly attempt to transact and have an interest in the contract. In a license-based show, nodes must be authorized and controlled to facilitate exchanges or in-series exchanges.

Binance launched the Soul Bound Token, also known as Binance Account Bound Token (BAB). It serves as an identity proof for users who have completed the KYC on the application. The main aim of SBT is to serve as identity credentials and with this user can also participate in airdrops and earn rewards and also work on new projects. This BAB token is nontransferable and therefore cannot be moved to other wallets and helps in verifying uniqueness of wallet. It is one per user and can also be revoked.

SBT's represent blockchain wallets and are issued by "Souls". This can also be used to represent any type of personal information of a person, for example, their medical records, resume, membership status and many more. SBT helps to revolutionize the concept of NFT's. It's not just about wealth and digital artwork or collectibles. It is one-of-a-kind token which represents a person or entity's reputation and has no monetary significance. This helps user in building digital, verifiable Web3 reputation on basis of their history and experiences.

SBT's help in tracking transactions and borrowing history of a user and other metrics. It helps in establishing trust in a trustless system of Web3 where user can own multiple wallets and participate in frauds and cybercrime. It also helps in preventing Sybil attacks. These are Blockchain's version of ID cards.

The concept of a decentralized autonomous organization (DAO) refers to online communities that unite for a shared goal and are governed by voting through smart contracts on a public blockchain. DAO's helps different communities in communicating and coordinating their operations but are still vulnerable to Sybil attacks.

A Sybil attack is a type of online security risk in which a single person attempts to take over the system by setting up numerous accounts, nodes, or devices. One person may easily accomplish this by opening several social media profiles. However, in the world of cryptocurrency, running numerous nodes on a blockchain network is a more relevant scenario. Sybil attack on E-voting system occurs when a single entity holds multiple wallets and tampers the voting result by acquiring 51% voting rights.

The concept of SBT was first introduced by Ethereum Founder Vitalik Buterin along with E. Glen Weyl and Puja Ohlhaver. It acts as foundation for the decentralized society or DeSoc.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

IV. IMPLEMENTATION

In this section we explain our proposed E-voting system that aims at solving the existing drawback in Blockchain-based E-Voting systems.

The proposed system contains a web application. Web application consists of a landing page, dashboard, polls, voting page and result page. Landing page is the main page where, when user is not connected to our system, the verification of the Soul Bound Token in the wallet takes place. Once authenticated user is redirected to the dashboard where they can see the ongoing polls. Once the user selects the poll, they will be redirected to voting page. At the end of the poll the result will be displayed at the result page.

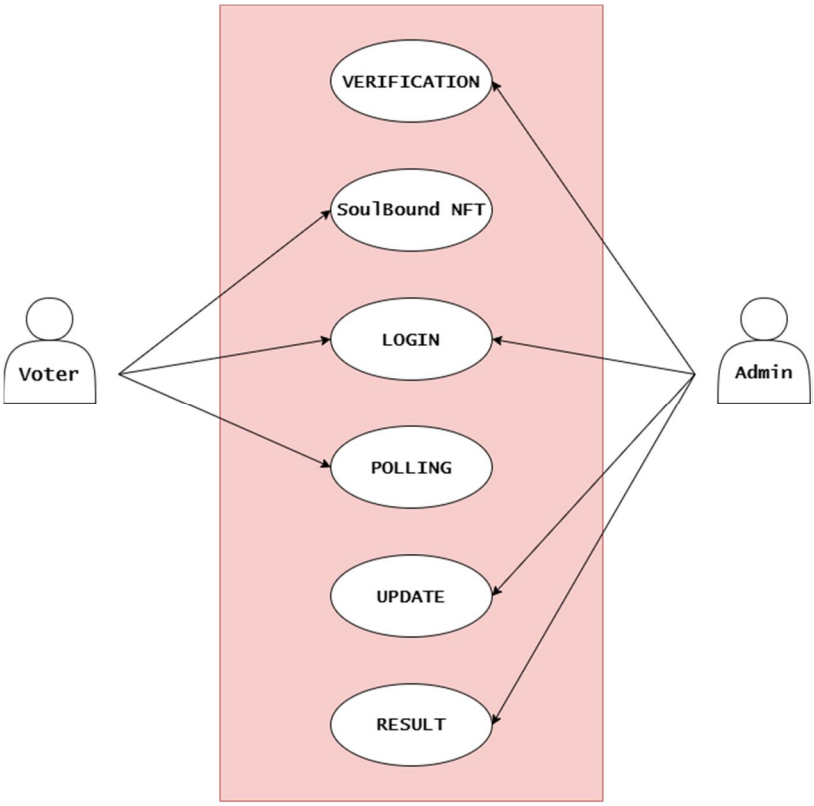


Fig. 1: Use Case Diagram

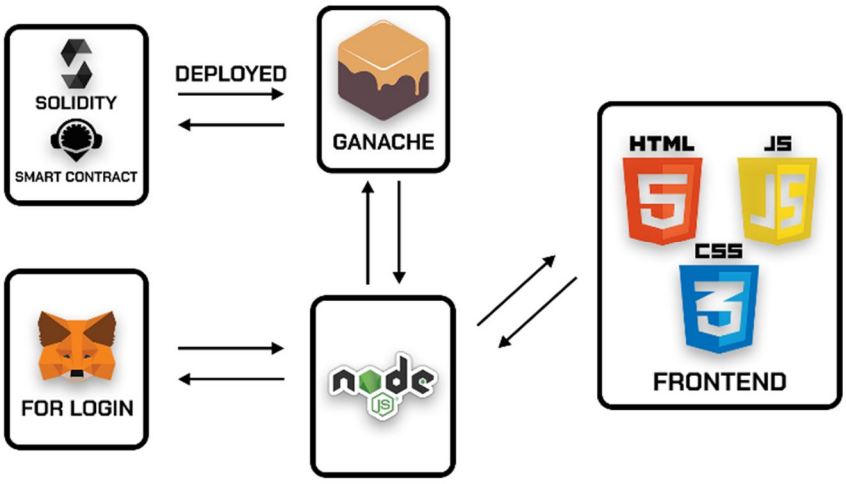


Fig. 2: Architecture

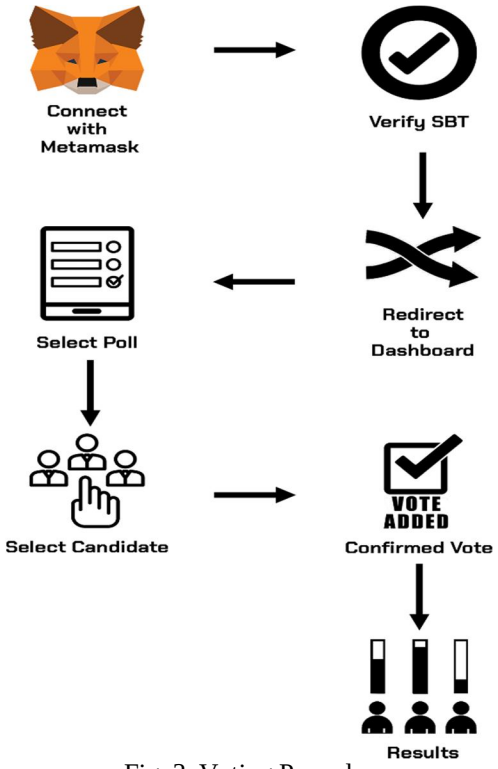


Fig. 3. Voting Procedure

SBTs are another substitute that has been put out for voting in decentralised autonomous organisations (DAOs). DAOs could issue SBTs that assign voting power based on users' engagement with the community rather than the existing governance approach, which is dependent on how many tokens a member possesses. BAB used in this system is a SBT minted by binance on Binance Smart Chain (BSC). It serves as unique id card for voters to access our system. The user can access our system only if they possess this BAB token in their meta mask wallet.

A software cryptocurrency wallet called MetaMask is used to communicate with the Binance smart chain network. Users can utilize a browser extension or mobile app to access their Ethereum wallet, which can then be used to connect with decentralized applications. This wallet contains the SBT.

The use of smart contracts offers a secure way to conduct voter verification, guarantee the accuracy of the results, make the voting system public, and guard against fraud. The voting contract is created once at the time of development and delivered by the Event Management Server several times with various questions and answers supplied by the event administrator as previously described.

A voter logs into the system by clicking the connect to metamask button. Once the button is clicked and a connection is established the system will verify the user. If the wallet connected contains the Soul Bound Token, then the user is granted further access to our system and their wallet address is retrieved. If the Soul Bound Token is not found then user cannot access our application.

Once logged in, the user will be redirected to dashboard where they can see all the ongoing polls they can access. From there they can select a poll and cast their vote to candidate of their choice. When the vote button is clicked, the voting smart contract will be deployed. It verifies all the necessary details. After successful verification a vote block will be created and is added to the blockchain. Within the voting application's blockchain, a valid vote is regarded as a transaction. A vote is therefore recorded in the blockchain as a new block. Only the one-person, one-vote principle is guaranteed by the system by using the voter's distinct SBT ID.

Voters can also track their votes using the transaction hash. At the end of the voting period, the result will be calculated and displayed.

The front end of the application is designed using HTML, CSS and ReactJS. The metamask wallet contains a Soul Bound Token named as the Binance Account Bound Token (BABT) whose contract address is 0x2B09d47D550061f995A3b5C6F0Fd58005215D7c8. The smart contract is made using Solidity and finally the transaction block is published to Ganache, which is a private Ethereum environment.

V. RESULTS

Since the 1970s, many versions of electronic voting have been utilized, and they have many advantages over paper-based methods, including more efficiency and fewer mistakes. Numerous efforts have been made to investigate the viability of using blockchain to support an efficient solution to e-voting in light of the phenomenal development in the use of blockchain technologies. This study has described one such endeavor that makes use of blockchain's advantages, including its transparency and cryptographic foundations, to create a workable e-voting system.

We analyzed and discussed the traditional voting system in this research, as well as the benefits of implementing a blockchain-based electronic voting system that makes use of various blockchain-based tools including SBT and smart contracts.

The use of blockchain as a voting method seems like an intriguing alternative. The blockchain industry is a continually changing ecosystem as new entities enter while others vanish. In fact, a growing number of research papers in the scientific literature suggest blockchain-based electronic voting applications. However, few of the suggested remedies have really been put into practice, and none have undergone extensive testing. Although the blockchain's underlying concepts are safe, e-voting systems are still susceptible to a number of threats. Given the stakes of such an application, it becomes exceedingly difficult to guarantee the integrity of an election.

In nations with sizable populations, blockchain-based voting apps for smartphones will enable a greater involvement of those who were previously cut off from the political process due to their remote location.

VI. FUTURE SCOPE

In future, we'll continue to implement or make adjustments to our system and also look into its potential performance. There are still some implementations, nevertheless, that can be used with our system.

Essentially, our objective is on creating an advanced and more effective method for electronic voting using blockchain technology and related variable tools. Also, we can use different SBT for different organizations and also provide different voting system to different organizations according to their personal needs.

REFERENCES

[1] Prof. Anita A. Lahane , Junaid Patel, Talif Pathan, & Prathmesh Potdar . (2020). Blockchain technology-based e voting system. Blockchain technology-based evoting. Retrieved from https://www.itmconferences.org/articles/itmconf/pdf/2020/02/itmconf_icacc2020_03001.pdf

[2] SAI CHARAN, PENTAPATI, & PREMA. (2022, March 3). A Research Paper on E-Voting Using Blockchain Technology. A Research Paper on E Voting Using Blockchain Technology. Retrieved from https://www.irjet.net/archives/V9/i3/IRJET V9I3167.pdf

[3] Shejwal , Gaikwad, Jadhav, & Nanaware . (2021, May 28). E voting using block chain Technology. E-voting Using Block Chain Technology. Retrieved from https://www.ijsdr.org/papers/IJSDR1905104.pdf

[4] Prof. M. Pathak, Suradkar, A., Kadam, A., Ghodeswar, A., & Parde, P. (2021, June). A Review on Blockchain Based E Voting System. ijsrst.com. Retrieved October 22, 9 C.E., from https://doi.org/10.32628/IJSRST2182120

[5] Jafar , U.; Aziz, M.J.A.; Shukur , Z. Blockchain for Electronic Voting System Review and Open Research Challenges. Sensors 2021, 21, 5874. https://doi.org/10.3390/ s21175874

[6] Kriti Patidar, Dr. Swapnil Jain (30 December 2019) Decentralized E Voting Portal Using Blockchain https://ieeexplore.ieee.org/document/8944820/citations#citations

[7] Yash Dalvi, Shivam Jaiswal and Pawan Sharma (2021, March 03) E-Voting Using Blockchain, Retrieved from https://www.ijert.org/

[8] S. Aruna, M.Maheswari and A. Saranya (2020) Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root, Retrieved from https://iopscience.iop.org/article/10.1088/1757-899X/993/1/012103

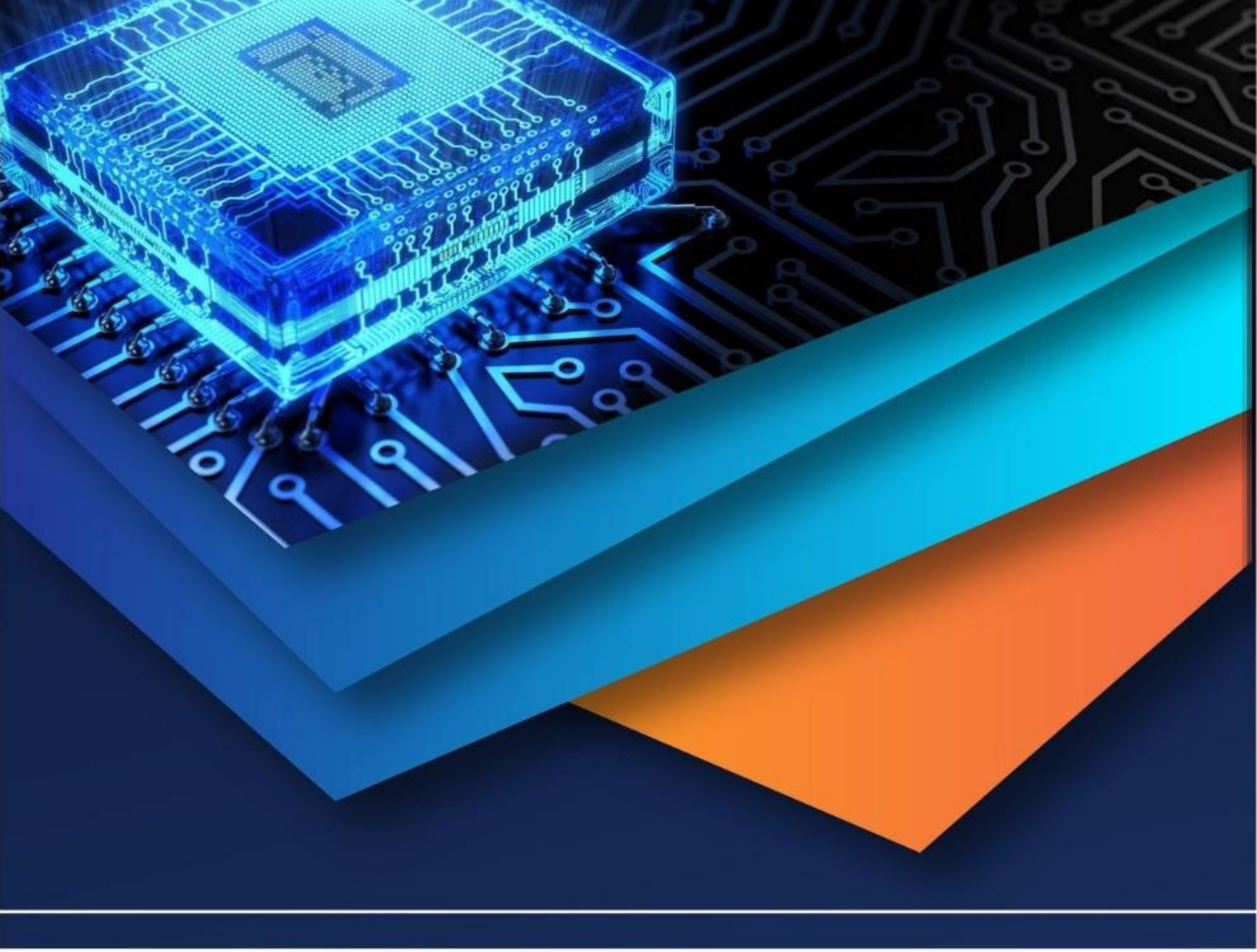
[9] Ali Benabdallah, Antoine Audras, Loius Coudert, Nour el Madhoun and Mohamad Badra (2022, July 1) Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review, Retrieved from https://ieeexplore.ieee.org/document/9812616

[10] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan (2018, May 1) Secure digital voting system based on blockchain technology, Retrieved from https://core.ac.uk/display/155779036?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

[11] Tanu Sri Kurakula, Rupa Sri Kurakula and Nikhita Pedamallu (2021 May) E-Voting System using BlockChain, Retrieved from https://www.researchgate.net/publication/351848054_E-Voting_System_using_BlockChain

[12] E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin(2022 May) Decentralized Society: Finding Web3's Soul, Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763

[13] Stefan Pieche (2022, September 8) Soul Searching, Retrieved from https://research.binance.com/static/pdf/Soulbound-Token-Stefan-Piech.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY