iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58239

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 II Feb 2024- Available at www.ijraset.com

Ox-Ethnio: Blockchain E-Voting System

Adarsh Maurya[1], Anupam Sharma[2], Mridul Srivastava[3], Arin Singh[4], Prof. Dinesh Kumar[5]
[1]*Department of Information Technology, KIET Group of Institutions, Ghaziabad, India*
[2]*Department of Information Technology, KIET Group of Institutions, Ghaziabad, India*
[3]*Department of Computer Science and Information Technology, KIET Group of Institutions, Ghaziabad, India*
[4]*Department of Electronics and Communication Engineering, KIET Group of Institutions, Ghaziabad, India*
[5]*Department of Information Technology, KIET Group of Institutions, Ghaziabad, India*

Abstract: ***In comparison to conventional paper-based systems, electronic voting, or e-voting, offers many benefits, including increased efficiency and fewer mistakes. It has developed into many different forms. However, gaining public approval of these systems remains a constant problem, especially when it comes to making them more resilient to possible weaknesses. With its potential to increase the overall resilience of electronic voting systems, blockchain technology is emerging as a market disruptor. With the use of blockchain technology, this project aims to create an efficient e-voting infrastructure by using its transparency and cryptographic underpinnings. The proposed technique satisfies the essential requirements for electronic voting systems and offers end-to-end variabilities essay delves into the planned e-voting mechanism and its actual implementation on the Multichain platform in great depth. Furthermore, Electronic voting systems, when applied in elections, need to uphold legality, accuracy, security, and convenience. Nevertheless, the potential challenges associated with digital voting methods can impede their widespread adoption. Blockchain technology has emerged as a promising solution to address these concerns, offering decentralized networks for electronic voting. Its main appeal lies in the ability to provide end-to-end verification, making it a preferred choice for developing electronic voting systems.***

I. INTRODUCTION

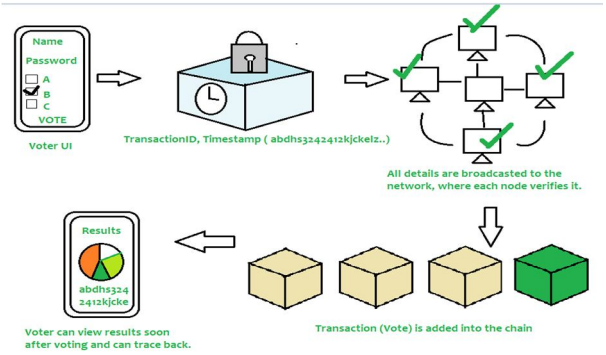
In any democracy, election security is critical to national security. Over the last decade, the area of computer security has attentively investigated the potential of electronic voting systems to lower the cost of holding national elections while also improving security safeguards. The conventional technique of democratic elections has depended on pen and paper throughout history. However, replacing this antiquated pen-and-paper system with modernized election technology is critical to reducing fraud and ensuring a traceable and verifiable voting process.

The conventional or paper-based polling approach increased people's trust in the majority vote process. It has contributed to the democratization of the democratic process and electoral system for choosing constituencies and governments.

It is critical to guarantee that voter confidence does not dwindle. A recent study indicated that the traditional voting procedure was not entirely sanitary, raising various concerns about justice, equality, and people's will.

II. BACKGROUND AND EVOLUTION OF BLOCKCHAIN E-VOTING PLATFORM

In the 1990s, Nick Szabo initially presented the idea of smart contracts Szabo posits that "smart contracts" are digital agreements enhanced with inherent protocols, enabling fulfillment by any two participating entities. Blockchain-based decentralized programs are essentially publicly accessible code. The execution outputs are separately validated by the users and a consensus mechanism. The steps incorporating blockchain technology and smart contracts are rendered

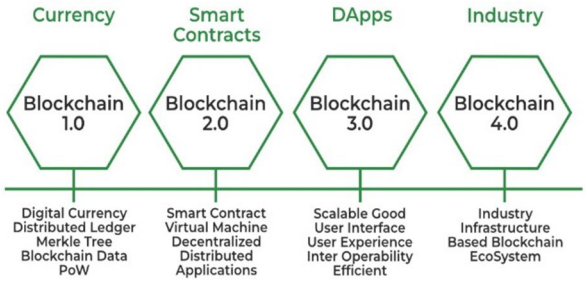


1) *The Genesis Phase:* This stage coincides with the inception of blockchain technology, which began with Satoshi Nakamoto's development of Bitcoin in 2009. The first blockchainbased digital currency that allowed peerto-peer trades without the need of middlemen like banks was Bitcoin.
2) *The Growth Phase:* At this time, blockchain technology gained more traction and several new blockchain projects with distinctive features and uses were developed. Moreover, Ethereum developed smart contracts in 2015, which are self-executing digital contracts. In the blockchain, smart contracts made it possible for business logic to be automated and for transactions to become more complicated.
3) *The Integration Phase:* As blockchain technology developed, more companies became aware of the potential advantages of implementing it in their operations. As a result, blockchain technology has been incorporated into a number of sectors, including banking, supply chains, healthcare, and more.
4) *The Interoperability Phase:* This stage of blockchain development focuses on the compatibility of various blockchain networks. This stage attempts to address the issue of blockchain fragmentation by making it possible for various blockchain networks to effortlessly connect and exchange data. In this stage, new technologies and protocols are also being created with the goal of facilitating interoperability between blockchain networks, such as Polka dot, Cosmos, and Ethereum 2.0.

We are just beginning to explore the potential of this ground-breaking technology, and the development of blockchain and smart contract transfer has been an overall interesting adventure. The potential for blockchain to disrupt business practises and change the global economy becomes increasingly clear as more sectors adopt the technology and new use cases arise.

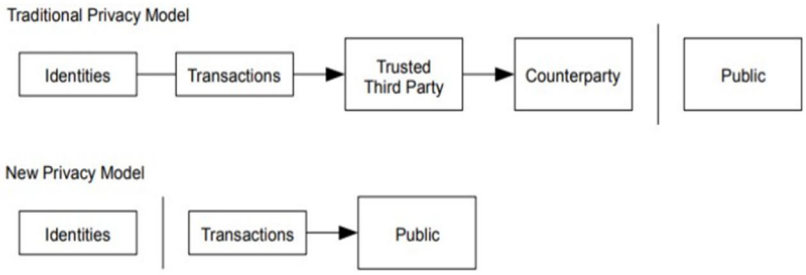
III. WHY BLOCK CHAIN IS IMPORTANT

Information is the lifeblood of business. It is great if it is received right away and promptly. Block chain is the ideal technology for distributing such information since it provides immediate, shareable, and completely transparent data that is recorded on an immutable ledger and accessible to authorized network users only. A block chain network has the ability to track sales, transactions, balances, and manufacturing, among other things. Moreover, since everyone has access to the same version of the truth, you can observe every facet of a transaction from start to finish, boosting your confidence and creating new opportunities.



A. Fraud and Attack Prevention using Block Chain

Block chain technology stops two internet crimes: duplicate spending and data hacking. By requiring miner nodes to accomplish computationally difficult tasks (referred to as "mining") to verify the payment, block chains address this problem. Infiltration, hacking, and breaches are a risk with centralised data storage and management systems, while a blockchain's distributed consensus mechanism makes hackers unable to access any information).



B. Blockchain Tools and Consensus Algorithm

Blockchain technology is powered by various tools and consensus algorithms that enable secure and transparent transactions. Here are some commonly used tools and consensus algorithms in blockchain:

1) Tools

- *Wallets:* A blockchain wallet is a type of electronic wallet that enables users to store, transmit, and receive cryptocurrencies and other types of digital assets.
- *Nodes:* Nodes are computers that use blockchain technology and take part in the transaction validation and verification process.

2) Blockchain Explorers

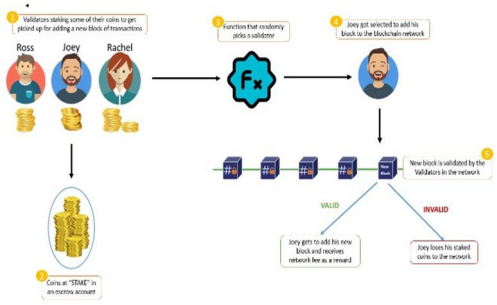
These are tools that let people observe and follow transactions on the blockchain.

- *Solidity,* a well-known programming language, is used to create smart contracts for Ethereum, however other blockchain systems may have their own specific smart contract languages.

3) Consensus Algorithms

- *Proof of Work (PoW):* This is the first consensus mechanism employed by Bitcoin, in which miners compete to solve a mathematical conundrum in order to approve transactions and add new blocks to the network.
- *Proof of Stake (PoS):* With PoS, validators are chosen to validate transactions and build new blocks depending on how much bitcoin they possess and "stake" as security.
- *Delegated Proof of Stake (DPoS):* In DPoS, the task of validating transactions and adding new blocks to the blockchain is delegated to a set of chosen validators known as "witnesses.".
- *Byzantine Fault Tolerance (BFT):* BFT is a consensus technique made to withstand and bounce back from malicious actors in a distributed system. On private blockchain networks, BFT is frequently employed.
- *Practical Byzantine Fault Tolerance (PBFT):* This BFT variation is tailored for high-performance blockchain networks.

In general, blockchain technology tools and consensus algorithms rely on the particular blockchain platform and its intended use case. We may anticipate the emergence of additional cutting-edge tools and consensus algorithms as blockchain technology develops.



IV. ELECTRONIC VOTING REQUIREMENTS AND THE PROPOSED SYSTEM'S ADHERENCE TO THEM

The general specifications for a common electronic voting system were created. Each criterion is briefly described below, along with an explanation of how the suggested solution complies with and meets each one.

Keeping the secrecy of each voter's vote is important for privacy. To maintain each voter's privacy, the suggested solution makes use of blockchain technology's cryptographic properties. In particular, the blockchain creates a special voter hash when a voter registers with the system, acting as the voter's unique identification inside the blockchain network. Importantly, the collision resistance feature of cryptographic hashing protects this identification from being misused. As a result, it is extremely difficult to track a vote, protecting voters, especially in circumstances where their vote may be in jeopardy.

Voting is only permitted by registered voters, and each voter may cast one vote To validate their ability to vote, the system requires all eligible users to register using special IDs, which are frequently official papers. This multi-layered strategy, which includes the use of biometrics, not only determines a voter's eligibility but also provides protection against instances of duplicate voting, preserving the fairness of the election process.

In conclusion, the suggested e-voting system successfully satisfies two important requirements: preserving voter privacy through blockchain cryptography and guaranteeing voter eligibility and singular voting through a combination of unique identifiers and cutting-edge authentication techniques, like fingerprinting technology.

V. EXISTING SYSTEM LIMITATIONS AND RESEARCH GAPS

There are numerous major obstacles and restrictions in the field of electronic voting systems that must be overcome:

A big technological difficulty is ensuring that prospective voters are accurately registered in the electoral system and that their data is in a digitally processable state. Furthermore, it is necessary to ensure the confidentiality and privacy of citizens identifying data.

Casting Anonymous Votes: It's important to keep voting online anonymously. Once cast through the system, every vote ought to stay private to everyone—including system administrators. This guarantees the confidentiality and accuracy of the voting process.

Individualized Ballot Processes: There is continuing discussion over the best way to represent votes in online applications or databases. Clear text communications are not the best option for maintaining anonymity and integrity, but hashed tokens can offer a workaround. The token solution makes it possible to relate a vote back to a specific voter, therefore maintaining the vote's non-reputability is a difficult task.

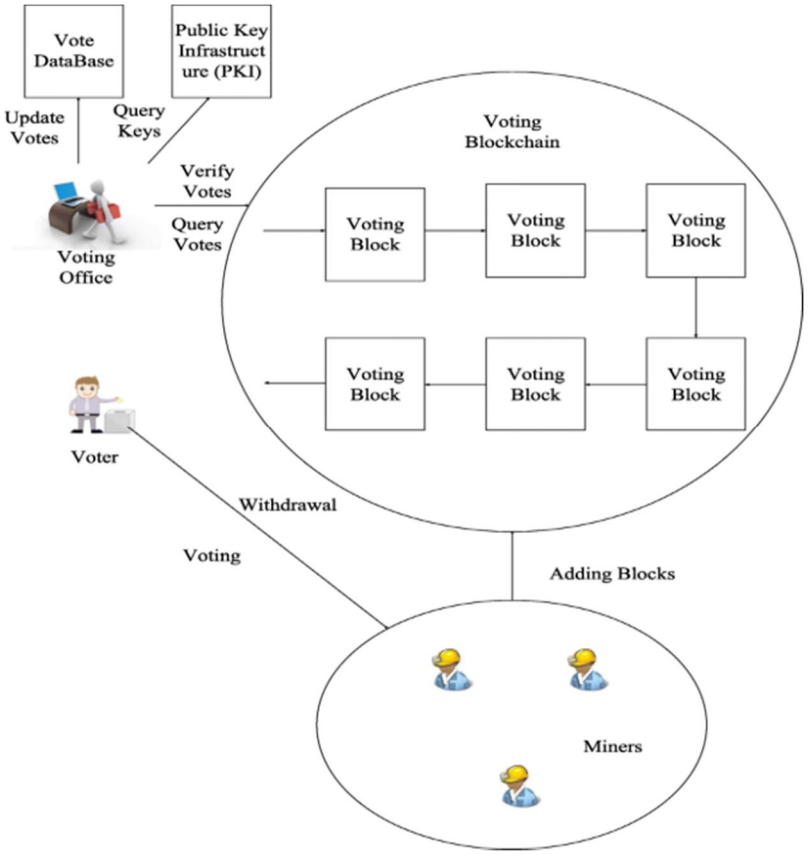
Voter Verifiability of Ballot Casting: During submission, voters should be able to examine and confirm their own ballots. This improves voter confidence in the process while also acting as a deterrent against any harmful operations.

High initial setup costs: Despite being typically cost-effective in the long term, online voting systems can be pricey to establish initially, especially for enterprises or organizations.

Growing Security Issues: Public elections are seriously threatened by cyberattacks. Real obstacles include DDoS assaults, hacking efforts, and worries about the accuracy of computerized voting equipment. Important security measures include preventing evidence erasure and providing openness with privacy.

Lack of Transparency and faith: It might be difficult to win the public's faith in the outcomes of online elections. In a completely digital process, it might be challenging to build perceptions of openness and reliability.

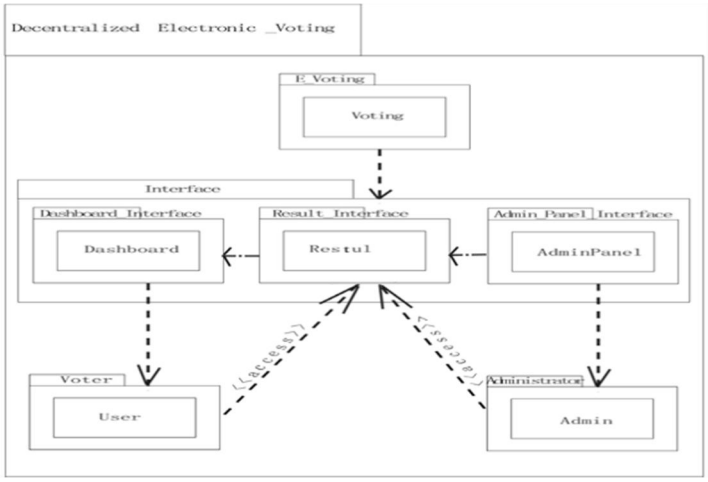
Voting delays or inefficiencies in remote voting: Synchronous remote voting requires stable and high-performing technological skills and infrastructure since timing is crucial in voting systems.



VI. OBJECTIVES AND THE PROBLEM

The goal of the project is to use blockchain technology to overcome these difficulties and restrictions associated with electronic voting. While preserving security and transparency, blockchain-enabled e-voting has the potential to reduce voter fraud and improve voter access. The main objectives are:

1) Integrating a safe mechanism for managing digital identities into the blockchain-based electronic voting system.
2) Ensuring anonymous polling while preserving the fairness of the election.
3) The creation of customized voting procedures that safeguard voter privacy and prevent vote fraud.
4) Establishing a method that can be verified independently so that voters may validate their ballots without jeopardizing security.
5) Investigating low-cost deployment techniques to lower the initial setup expenses of blockchain-based electronic voting systems.
6) Improving security measures to protect against cyberattacks and guarantee the integrity of evidence.
7) Use blockchain technology to render the electronic voting process transparent and trustworthy.
8) Making remote voting more synchronous as well as trustworthy by optimizing it to reduce delays and inefficiencies.

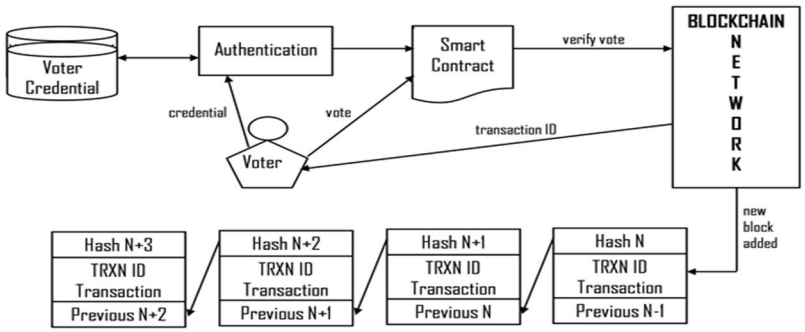


The research intends to contribute to the creation of a safe, transparent, and reliable blockchain-enabled e-voting system that may be successfully applied in a variety of election situations by addressing these issues and objectives.

VII. OVERCOMING THESE CHALLENGES

1) *Enhancing Transparency and Verifiability:* The voting process must be made open and transparent in order to make it simple for the general public to inspect it and confirm the fairness of the election.
2) *Vote Accuracy and Security:* It is essential that the voting system ensures the precise and secure recording of every vote cast by a voter, eradicating the chance of fraud or miscounting.
3) *Eligibility Verification:* Only qualified voters should be permitted to vote. The system must utilize dependable mechanisms to guarantee that voters are eligible. By designing the election system to be tamper-proof, unauthorized parties will find it exceedingly difficult to meddle with or influence the voting process.
4) *Preventing Influence from Powerful Entities:* The system should be structured to prevent powerful groups from unlawfully leveraging their influence or rigging elections. These essential needs may be successfully met by implementing blockchain technology:
5) *Authentication:* Blockchain strengthens the security of the system by ensuring that only registered voters may take part in the election. Voter privacy is protected by blockchain technology, which ensures that votes cast and voter identities are kept separate. Votes cast and recorded on the blockchain become immutable, prohibiting any unlawful tampering or change.
6) *Verifiability:* The blockchain-based technology makes it possible to transparently verify the number of votes cast, fostering trust in the electoral process.

In finalization, the main objective is to design a blockchain-based electronic voting system that not only satisfies the necessary specifications but also acts as a robust, secure, and transparent platform to solve the issues of voter fraud and improve voter access



VIII. FRAMEWORK FOR THE PROPOSED SYSTEM

Our suggested e-voting technique is modeled after the well-known Prêt à Voter e-voting strategy described in Ryan's 2008 study. This system has been carefully designed to suit the strict requirements of real-world voting situations, guaranteeing crucial elements like privacy, eligibility, ease, receipt-freeness, and verifiability. Our main goal is to deliver a safe digital voting experience without sacrificing usability.

We created a web-based interface with a smooth and user-friendly user experience to achieve this goal. We have also strengthened the system's general security by implementing fingerprinting procedures to avoid instances of duplicate voting. We have included a user-friendly administrator interface for simple access and administration since we recognize the need for effectively managing voters, constituencies, and candidates.

A fair and competitive atmosphere for all candidates is fostered by our system, which is also built to provide equal voting rights for all qualified participants while protecting voter confidentiality. Voters receive an email with the cryptographic hash of their transaction ID as verification of their cast vote as an additional degree of protection. Even beyond the boundaries of the voting constituency, this hash may later be utilized for verification for various reasons.

IX. CONCLUSION

The objective and overall study of this research paper is to investigate and evaluate research concerns to EVS(election voting system) based on block chain technology. The article tells us about recent research on blockchain based electronic voting(EV),starting by exploring the blockchain concepts and it's application.

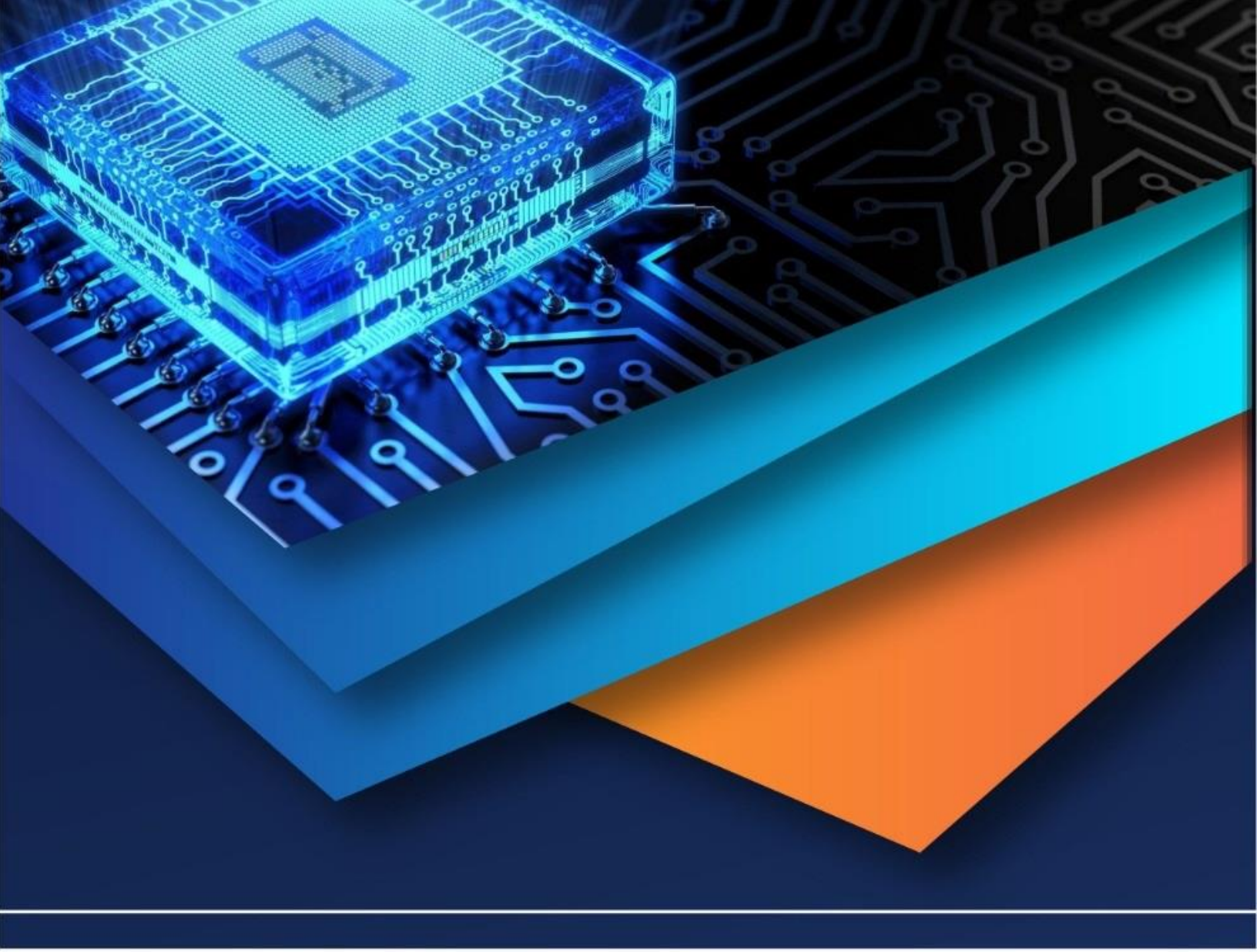
Afterwards, it examines the current electronic voting system methods, concedes their limitations and proposed solutions. Identifiable considerable potential of blockchain to intensify electronic voting, the article also discussed existing solutions for blockchain based electronic voting and highlights latent research directions in this domain. According to several experts, block-chain seems fitting for decentralized electronic voting systems(EVS).

In contemporary society, the idea of leveraging digital voting technologies to make public voting more cost-effective, efficient, and user-friendly holds considerable appeal. Moreover, it enables a more direct form of democracy, allowing individuals to express their opinions on specific laws and proposals.

REFERENCES

[1] Taherdoost, H. (2023, February 13). Smart Contracts in Blockchain Technology: A Critical Review. MDPI. https://doi.org/10.3390/info14020117
[2] Virani, H., & Kyada, M. (2022, December 9). A Systematic Literature Review on Smart Contracts Security. arXiv.org. https://arxiv.org/abs/2212.05099v1
[3] Benny, A. (2020, August 11). Blockchain based E-voting System. Blockchain Based E-voting System by Albin Benny:: SSRN. https://doi.org/10.2139/ssrn.3648870
[4] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021, April 18). Blockchain smart contracts: Applications, challenges, and future trends. PubMed Central (PMC). https://doi.org/10.1007/s12083-021-01127-0
[5] Hoffmann, T., & Skwarek, V. (2019, May 20). Blockchain, Smart Contracts und Recht. Informatik Spektrum, 42(3), 197–204. https://doi.org/10.1007/s00287-019-01180-3
[6] Haney, B. (2023). Defining Smart Contracts. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4574563
[7] Prause, G. (2019). Smart Contracts for Smart Supply Chains. IFAC-PapersOnLine, 52(13), 2501–2506. https://doi.org/10.1016/j.ifacol.2019.11.582
[8] Smart Voting Platform (Secured Digital Voting System) Uses Blockchain Technology and Biometric Authentication. (2023, May 17). International Journal of Science and Engineering Applications, 105–113. https://doi.org/10.7753/ijsea1205.1029
[9] Javaid, M. A. (2014). Electronic Voting System Security. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2393158

[10] DECENTRALISED ONLINE VOTING SYSTEM. (2023, May 31). International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets40446
[11] Mayuri Gomte, Harshal Chaudhari, Abhishek Tapare, & Dr. Y. M. Patil. (2023, April 28). IoT Based E-Voting System to Avoid Fraud Voting. International Journal of Advanced Research in Science, Communication and Technology, 289–293. https://doi.org/10.48175/ijarsct-9576
[12] Yao, J., Wei, L., & Liu, T. (2020, July 6). Blockchain-Based Voting System. Computer System Networking and Telecommunications, 3(1). https://doi.org/10.18063/csnt.v3i1.1146
[13] Khan, I., & Shahaab, A. (2021, February 2). A Peer-To-Peer Publication Model on Blockchain. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.615726
[14] Enguehard, C. (2019, July 8). Blockchain and Electronic Voting. Terminal, 124. https://doi.org/10.4000/terminal.4190
[15] Bartoletti, M. (2020, June 4). Smart Contracts Contracts. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00027



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY