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.2024.58856

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

Analysis of Coercion-Resistant for E-Voting System based on Blockchain

P. V. V. S. Eswar Rao[1], Tanveer Sheik[2], Sabhiya Shaik[3], Dhanunjaya Kandula[4], Navya Sri Kodamanchili[5], P. Siva Kumar SMIEEE[6]
Computer Science and Engineering, Sasi Institute of Technology & Engineering, Tadepalligudem, India

Abstract: ***Election absenteeism rates are steadily rising, partly a result of the distance required to cast a vote. The use of electronic voting procedure would eliminate the need for travel and enhance voter turnout. In addition, compared to the conventional paper ballot voting technique, this reduces dangers like manipulations and produces results more quickly. A remotely electronic voting system should, nevertheless, adhere to the highest standards of security, dependability, and transparency given the significance of an election. Numerous remote e-voting systems, many of which are based on blockchain technology, were examined in this literature review. Blockchain technology provides for the removal of the Trusted Third Party (TTP) and the decentralization of transactions while also providing transparent and completely secure data storage, making it a new technical foundation for many different types of IT applications. The use of smart-contract technology, which automates and executes user agreements, is also permitted. The authors of this study examine the most insightful blockchain-based e-voting options. The lack of openness and auditability in conventional voting methods can be addressed by blockchain technology. A reliable computing platform is offered by running a self-enforcing e-voting system on a blockchain for real-time data verification.***

Keywords: Blockchain, E-Voting, Smart contract, Ethereum, Encryption/Hashing.

I. INTRODUCTION

As Democratic voting is very critical in any country due to lack of transparency. It is challenging to win over voters in traditional voting systems because voting machines connected to centralized databases can be tampered with and manipulated by someone with physical access to the equipment [1]. The choice of voters should be based on free will [2].

Blockchain becomes the most popular technology in providing the security, privacy, transparency. The immutable, decentralized blockchain limits the illegal access to change the data in its applications and also it provides integrity and confidentiality for its applications [3,4]. Blockchain is a technology of a digital ledger in which the data or transactions can be stored in the blocks without the need of any third-party are linked together in the network to form a chain. It is known for its capacity to offer a safe and clear way of storing and sharing data, making it the best choice for e-voting systems. [5]. However, the real voter could not confirm that their vote was reflected in results [6].

Indeed, Online Voting already took place in various nations for minor elections, yet, it remains cautious. The hazards of assaults are also significant, limited expandability like voting procedures doesn't but enable us to contemplate it for nationwide election. The procedure remains, like physical election, exceedingly intricate to authenticate and examine for a voter who lacks control over the electoral process. To surpass issues, blockchain emerges as an encouraging technology [7][8]. A growing number of software applications are being created on the blockchain, a nascent technology that hasn't yet reached its full potential. Many initiatives that demanded a system to store and share data without passing via a Trusted Third Party (TTP) have utilized it because of its distributed, anonymous, and secure nature [9].

Blockchain based voting system achieves coercion resistance and receipt-freeness and also it is impossible to gain access to all the votes without taking control of entire network [10]. It connects users to the network and maintains growing data records protected from unauthorized manipulation, tampering [11]. Using a distributed application allows the voting system to offer fairness and flexibility during the election period than existing system [12]. Open Vote Network is a self-tallying protocol implementation that provides the highest level of voter anonymity [13,14]. Also found that blockchain technology can provide a tamper-evident and auditable voting system that is resistant to manipulation [15].

In this article, we analyze the most insightful blockchain-based electronic voting technologies to better understand their unique features and what advantages they have over conventional voting. Our strategy was to learn as much as we could about the current status of concerning electronic voting and blockchain technology.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Then, we took a few characteristics that were common to most blockchain-based electronic voting apps. By categorizing the comparison criteria into many distinct themes: voting encryption/hashing methods, opposed to assaults, as well as security features, we were able to create a subset of comparison criteria.

The remainder of the essay is structured as follows: The Background study is presented in Section II. The Related work is presented in Section III. Analysis and Discussion are covered in Section IV. Future work is covered in Section V, which concludes the essay.

II. BACKGROUND STUDY

A. Blockchain Technology

Blockchain technology has emerged as a revolutionary concept in distributed ledgers, dramatically changing the way stakeholders communicate and exchange information. At its core, blockchain empowers individuals or organizations exchange information directly without the need for prior knowledge or trust. Each is sealed with cryptographic signatures to prevent any attempts to tamper the data.

Every block has the previous record's hash in it, which is subsequently correctly inserted into the block's data header. This clever design keeps the parts dependent on each other, making any changes to the records in the chain more efficient in computers. Simply put, changing one record snaps the entire chain, alerting participants to any bad play.

But for blockchain to work properly and provide participants with a valid chain of control to ensure data integrity, consensus among participants is needed A consensus protocol works as the glue that binds the blockchain network, allows participants to collectively agree on transaction integrity and maintain a harmonized, tamper-resistant ledger Being enabled This key feature ensures that underlying blockchain principles a with trust, security and transparency following in practice.

B. E-Voting system

E-voting, short for electronic voting, is a modern and technologically advanced method of casting and counting votes in elections and other democratic processes.

It replaces traditional paper ballots with digital systems, and provides eligible voters ability to use computers, tablets, smartphones and other electronic devices Benefits, such as increased access for voters with disabilities, faster and more accurate vote counting, and the possibility of remote voting can drive voter turnout high but will also raise concerns about security, privacy, and possibility of computer sabotage/hacking.

C. Smart contract

It is a dynamic set of code and data that works on an EVM. These contracts alone have the power to govern and bind their terms in part or in whole. The lifecycle of a smart contract generally comprises of three basic steps: It is blockchain allows multiple users to enter into collective agreements, often coded in a language like Solidity. Second step is to place the smart contract on the network chain.

With this implementation, contract is made available to each peer-to-peer (P2P) network node and assigned unique address on the blockchain.

Hence, it is implemented automatically, based on predefined conditions. These scenarios are usually based on actual events or data entry.

When a contract works, it generates transactions on the blockchain, recording the consequences of its actions. These duties are irreversible and traceable, ensuring transparency and accountability in the operation of the contract.

Smart contracts, with their automation and traceable transactions, are changing the way contracts are negotiated and executed in the digital realm.

Figure 1 demonstrates how the current voting system operates, in which requires voters to get verified by getting the voter ID card after the verification from the authorities the voters are allowed to cast vote in allocated ballot box. They cast their votes at polling station which is secured by the armed forces all over the polling station. The polling station is maintained by the central authority and provides the needs and services by the polling station. After voters casted their votes, will be sent to the central authority to announce the result.

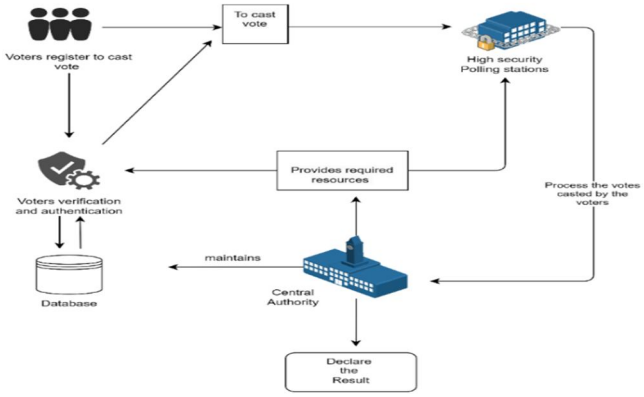


Figure 1: Traditional Voting system

Figure2 shows the procedure of electronic voting by system using the blockchain technology, in this the voters were verified and authenticated first from the database of the registered voters. Then voters cast their ballots using web application that can work on either electronic device such as mobiles, laptop/desktops.

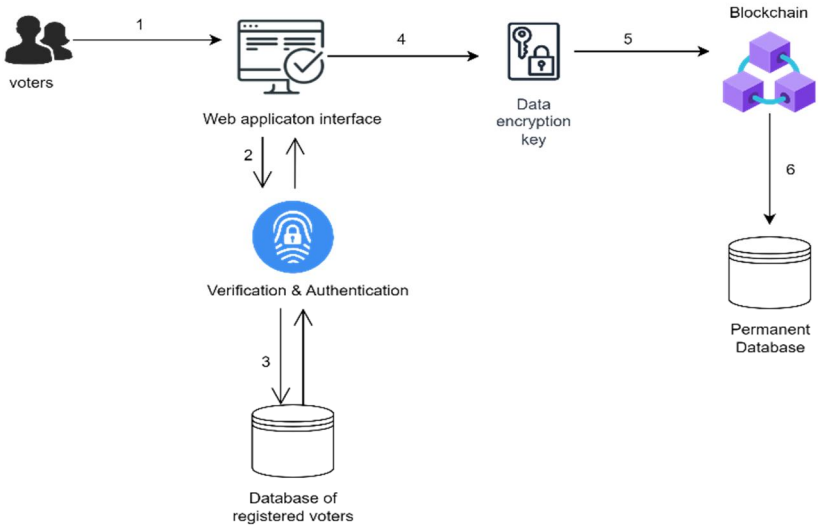


Figure 2: Electronic voting system

III. RELATED WORK

A. Public blockchain and Ethereum

Public blockchains is completely open to the idea of decentralization, providing an inclusive and transparent platform that extends beyond the realm of cryptocurrencies, with Bitcoin and Ethereum leading the charge in. These dynamic networks rely on array of nodes, validating the transactions, and protect the immutable ledger from tampering. Security, the cornerstone of the public blockchain, is enabled by sophisticated cryptography techniques and imaginative techniques such as the respectable PoW or the evolving PoS. It reinforces it.

Fatima *et al.* [16] addressed vulnerabilities in centralized systems, such as cyberattacks, data manipulation, and privacy breaches, by proposing a decentralized Ethereum e-voting system. To overcome issues in regular voting methods by introducing a decentralized application (dApp) for remote voting [17], potentially enhancing efficiency and reducing costs. Proposed [18] a new Open Vote-Network (OV-Net) that is more safer for more candidates. This alternative used an automatic counting method without revealing his or her vote. Although their design showed promise [19], yet another test and device safety considerations are important for real-world applications. The potential of decentralized voting on Ethereum's blockchain [20] needs the practical use of resources and the creation of defenses against possible attacks were still important considerations.

A promising solution to the challenge of electronic elections, with a secure, transparent, and effective system that encouraged devolution of constituencies [21] although theory should be considered types of voter availability, understanding, and fidelity for real-world use though. In [22] a new e-voting system combining blockchain and IPFS technologies for security and cost savings was introduced. 5G wireless networks were used to improve connectivity, and efficiency was achieved. Performance analysis of the Ethereum test network revealed benefits such as voter privacy protection, reduced certificate compromise, and independence from third-party authorities but the authors acknowledged if the system requires an Internet connection it is complex and potentially vulnerable to cyberattacks. Although it showed strength in a variety of areas, further research was needed in terms of measurement and adaptability [23].

In [24] worked on the combination of blockchain and IoT for secure voting in smart cities, providing improved security and transparency. Darren Thebes *et al*. [25] worked on and presented the use of Architecture Trade-off Analysis Method (ATAM) to assess blockchain e-voting system design in a specific national context, engaging stakeholders and providing valuable insights but having to measure methodology of resource requirements and knowledge bases in its implementation.

The work of J Arshad *et al.* [26] shed light on the issues associated with transaction manipulation attacks on blockchain e-voting applications. According to Michal Pawlak *et al.* [27] research provided valuable insights into the state of blockchain-based electronic voting systems. Although the findings were insightful, further research and extensive usability testing were needed to better understand the impact of attacks. However, the exclusion and limited availability of the gray literature must be considered when assessing the generalizability of the findings.

Shiyao Gao *et al.* [28] discussed a certificateless traceable ring signature algorithm that verified public key certificates and enabled auditing of the e-voting process. The e-voting protocol was supported by blockchain technology, which ensured the fairness and transparency of the voting process and results. The experiment was conducted by simulating the e-voting protocol using Python and analyzing its security and efficiency. The proposed protocol achieved the basic requirements of e-voting, including anonymity, transparency, fairness, and security against quantum attacks.

Dong Zheng *et al.* [29] concluded challenges facing traditional e-voting systems including lack of data, security and confidentiality, and the possibility of coercion and vote buying They proposed a smart blockchain-based E-voting system to ensure that integrity, fairness and protection of confidentiality -implementing agreements. A detailed presentation was given on the computational theory and cryptographic techniques used in the system, and security modeling & performance analysis Blockchain technology ensures security and transparency, and fairness of the system using smart contracts, all of which are features of it necessary for fair and safe elections but this system is not scalable.

A completely electronic voting system that passed the Gateshead trial's end-to-end verifiability test is shown in [30]. The research suggests using a fully E-voting system that is E2E verifiable, allowing voters to check the efficiency and ensuring the fairness of electoral method. 94 voters took part in the Gateshead trial, casting 93 valid ballots and 11 invalid ballots. According to the report, the Gateshead trial participants clearly preferred verified electronic voting over conventional paper ballots. The fact that 22% of participants still preferred or strongly favoured paper voting highlights the need for caution and support for voters who could be unsure about or opposed to e-voting.

In E. Zaghloul *et al.* [31] provides a thorough investigation of privacy and security challenges connected with Bitcoin and blockchain technology. It evaluates double-spending attacks, major network security attacks, security issues in Bitcoin storage wallets, and privacy limitations inherent in the Bitcoin system.

In [32], a distributed ElGamal cryptosystem, a keyed-Hash Message Authentication Code (KHMAC), Decisional Diffie-Hellman (DDH), or a non-interactive zero-knowledge proof (NIZKP), multifactor authentication, digital signature scheme, and zero-watermarking are used to create a a reliable and secure electronic voting system. The creation of polling tags, the use of zero-watermarking for polling, and the construction of a three-layered authentication mechanism are some of the paper's novel results.

In [33] described the usage of cryptographic primitives, utilizing a distributed ledger, and blockchain integration. The advantages of using blockchain in e-voting systems include transparency, immutability, decentralized control, and the ability to preserve verifiability. However, there are limitations to using blockchain in e-voting systems, such as scalability issues, potential privacy concerns, and the need for robust consensus mechanisms. Some studies propose blockchain-based e-voting systems, while others argue against it due to security risks and limitations.

To increase the voting process's integrity, transparency, and security, research on these issues has been done and used in E-voting systems like Ques-Chain [34]. Blind signatures and Ethereum-based smart contracts are proposed methods to address challenges in e-voting systems.

The use of cryptographic techniques such as zero-knowledge proofs, range voting, and secret sharing. Experiments have been conducted to evaluate the effectiveness of blockchain-based self-tallying voting systems, such as PriScore [35], which demonstrated maximum ballot secrecy. Limitations include reliance on cryptographic techniques, which may introduce complexity and potential vulnerabilities if not implemented correctly, and scalability issues.

Voting technologies built on the blockchain, such ACB-Vote [36], are intended to increase voting's efficiency, security, and transparency. In order to avoid duplicate voting by anonymous voters, the ACB-Vote score voting system uses convertibly linkable signatures on the blockchain. Heavy range proofs are avoided, batch ballot verification is supported, and a variety of tallying techniques are made possible by the system. BBS+ signature and knowledge signatures are used to protect ACB-Vote's security. The innovative results of ACB-Vote include its capacity to offer effective and adaptable score voting while safeguarding privacy. The benefits of blockchain-based voting systems include their enhanced transparency and immutability, reduced election expenses, and increased efficiency in counting votes.

To make voting procedures more dependable and secure [37]. Privacy disclosure, casting multiple ballots, and abstention are issues. There has been a proposal for a new voting system that uses threshold secret sharing technology to address issue of voting by abstentions and a range proof mechanism to confirm that the ballot is legitimate. The proposed scheme achieves security intensity and scalability. Advantages include decentralization, immutability, non-reputability, transparency, pseudonymity, and traceability. Limitations include storage of paper ballots, verification by voters, scalability, and efficiency.

On blockchain-based applications in various domains, including education and banking [38]. The review discusses the challenges, proposed methods, experimental approaches, unique findings, advantages, and limitations of blockchain technology. A overview was provided on the applications and tools used in blockchain, including Ethereum.

Applications in various domains, including academics and education, banking, and healthcare, examination, certificate, and transcript system for education, Interbank Spunta project for banking [39]. A decentralized architecture to address academic misconduct. Results indicate that the suggested strategy will work as secure, efficient, scalable, making it suitable for large-scale voting [40]. As a limitation, system does not satisfy non-coercibility, as voters can validate their votes by displaying the keys used during the voting and counting processes [41].

B. Private blockchain

Simona-Vasilica Oprea *et al.* [42] emphasized a solution optimized for university elections. It effectively addressed various challenges while providing transparency and security. The work of Ruhi Tas *et al.* [43] introduced a two-layer encryption model to address the data-related challenges. While the testing showed promise for enhancing security and privacy, further research into real-world applications and scalability considerations needed to be done.

A system that used efficient hashing techniques and associative using blockchain to secure privacy and security of electronic voting data [44]. The study used the consortium's blockchain to ensure that the blockchain belonged to the governing body, and to prevent unauthorized access from the outside, the study also used effective hashing techniques to ensure electronic voting information is secure.

The proposed system introduced the concept of a block ceiling, helping it to be flexible to the voting system's requirements. Security and reliability of the system are advantages of the method. However, the study was conducted theoretically, and it was not clear how the proposed system would work in a real situation. Furthermore, the paper didn’t provide any evidence to support the effectiveness of the proposed system and does not address the issue of accessibility to people with disabilities, an important concern in computing so elections in Prevention shown promise.

Access control procedures [45] may call for the storing of passwords or biometric templates, which is incompatible with the decentralized environment of blockchain, which might disclose sensitive information of the parties involved. Various methods have been proposed to address multi-channel approaches, privacy-preserving software update protocols, and blockchain-based access control frameworks.

A peer-to-peer implementation [46] for many developing blockchain-based applications in a number of industries, such as banking, e-voting platforms, storage and data protection, reputation management, smart contracts, the internet of things, healthcare, and transportation.

MAS-Encryption (MASE), to guard the secrecy ofmultiply-add (M-A) classifiers type. They demonstrated the effectiveness of MASE through two case study [47] examples: constructing a privacy preserving Naive Bayes classifier with minimal Bayes risk (MBR-PPNBC) and a privacy-preserving support vector machine classifier (PPSVMC).

Auditable Blockchain Voting System (ABVS) system integrates [48] blockchain technology and utilizes intelligent agents and multi-agent systems to offer advantages such as transparency, verifiability, and reduced risk of fraud. The advantages of MASE, a cryptographic tool for privacy-preserving classifiers, include its ability to handle input and secure computation on M-A structure, while minimizing communication overhead and computation time. The system guarantees fairness and confidentiality while meeting the security requirements for establishing transactions and encrypting vote data [49]. The simulation involved 10,000 nodes and 100,000 voters. The outcomes demonstrated the system's capability is to handle a large number of transactions simultaneously and was resistant to various types of attacks, including Sybil attacks and double-spending attacks [50].

IV. ANALYSIS AND DISCUSSIONS

The security requirements of the blockchains used in various electronic voting systems will be analyzed and discussed in this section. In order to demonstrate the detailed operation of voting system and how voters choose the victor in elections, various similar e-voting protocols are contrasted and analyzed in the final step. For which we have several smart contract functionalities set up for various voting systems.

The following section relate the main subject areas to the proposed blockchain-based e-voting applications: (A) Various implementations, (B) Encryption/Hashing algorithms.

A. Various *Implementations*

The general voting procedure is the same across all blockchain-based electronic voting programmes, from registration to announcement of the outcome. After quickly outlining the overall functionality of electronic voting in this section using blockchain, examined few of the dynamic components of the various approaches discussed.

1) *Such as:* Initialization- During this stage, the voting procedures, voter list, and candidate list are initialised into the smart contracts.
2) *Authentication:* Various authentication procedures allow users to login and identify themselves on election day. On occasion, a specific website or programme is utilised.
3) *Voting:* Voters choose their candidate, accordingly then votes are encrypted/hashed using Encryption/Hashing algorithms.
4) *Counting & Result:* Counting of votes takes place in parallel results of the election are made public at the final point.

B. *Encryption/Hashing Algorithms*

1) *SHA-256:* SHA (Secure Hashing Algorithm) is one of the most popular hash algorithms, which belongs to SHA 2 family of algorithms that always produces the final hash digest value as 256 bits.
2) *Homomorphic Encryption:* The homomorphism encryption feature enables operations on ciphertexts without having to first decode them. This characteristic enables encrypted votes to be tallied by the third party in a voting system without any data on the ballot being revealed. The Paillier and ElGamal homomorphic cryptosystems, which allow for an infinite number of modular additions and multiplications, respectively, are frequently used in voting systems.
3) *Zero Knowledge Proof:* ZKP is a cryptography protocol used to ensure privacy, security, and end-to-end verifiability. ZKP allows a prover to prove the truth of a statement without revealing the statement's contents or how the truth was discovered. ZKP-based blockchain voting systems offer tamper-proof and secure voting systems, utmost privacy and confidentiality, and efficient.
4) *Blind and Ring Signature:* While using a digital signature, the message's content is first masked (or "blinded"). The message is initially "blinded" by fusing it with an unpredictably generated "blinding factor". A signer receives the blindfolded message and signs it by applying a common signature algorithm. The resultant message may then be checked against the signer's public key combined with the blinding factor. Without explicitly identifying themselves, a user who belongs to a specified class of users can access a certain resource. To demonstrate that the resource has been accessed, third-party verifiability may be necessary. can be used in designated-verifier signatures, particularly in emails.
5) *Ethereum Hash Function:* Keccak-256 is a cryptography hashing function that is used in the Ethereum blockchain to calculate the hashes of Ethereum addresses, transaction IDs, and other significant information in the Ethereum ecosystem. It belongs to the SHA-3 family of hash functions, which won the 2012 NIST hash function competition. Keccak-256 is meant to be resistant to a variety of assaults, such as preimage attacks, collision attacks, and length extension attacks. With a relatively modest computing cost and a straightforward implementation, it is also effective.

TABLE I. ANALYSIS OF ETHEREUM BLOCKCHAIN

Ref.no	Blockchain	Security criteria		Encryption/hashing algorithms
		Coercion-resistant	Scalability	
Fatima *et al.* [16][2023]	Ethereum	✓	×	Keccak256
Anitha *et al.* [17][2022]	Ethereum	✓	✓	Ring signature
Sangsoo *et al.* [18][2022]	Ethereum	×	×	Zero Knowledge proof
Ehab *et al.* [19] [2021]	Ethereum	✓	✓	Blind signature
McCorry *et al.* [20] [2021]	Ethereum	✓	×	Blind signature
Feng Hao *et al.* [21] [2021]	Ethereum	✓	×	Zero Knowledge proof
Razu *et al.* [12][2020]	Ethereum	✓	×	SHA-256

TABLE II. ANALYSIS OF PUBLIC BLOCKCHAIN

Ref.no	Blockchain	Security criteria		Encryption/hashing algorithms
		Coercion-resistant	Scalability	
Shail *et al.* [22] [2023]	Public blockchain	ü	û	SHA-256
Huilin *et al.* [23] [2022]	Public Blockchain	ü	ü	Homomorphic Encryption
Junaid *et al.* [26] [2020]	Public blockchain	û	û	SHA-256
Darren *et al.* [25] [2020]	Public blockchain	û	û	SHA-256
Michał *et al.* [27] [2021]	Public blockchain	ü	ü	Blind & Ring signature
Dong Zheng *et al.* [28] [2020]	Public blockchain	û	û	Ring signature algorithm
Shahzad *et al.* [44] [2020]	Consortium blockchain	ü	û	SHA-256

In the table1, table2 we have compared and analyzed several different Ethereum and public, private blockchains to check whether the given blockchain provides the coercion-resistant and scalability, while using the encryption/hashing algorithms.

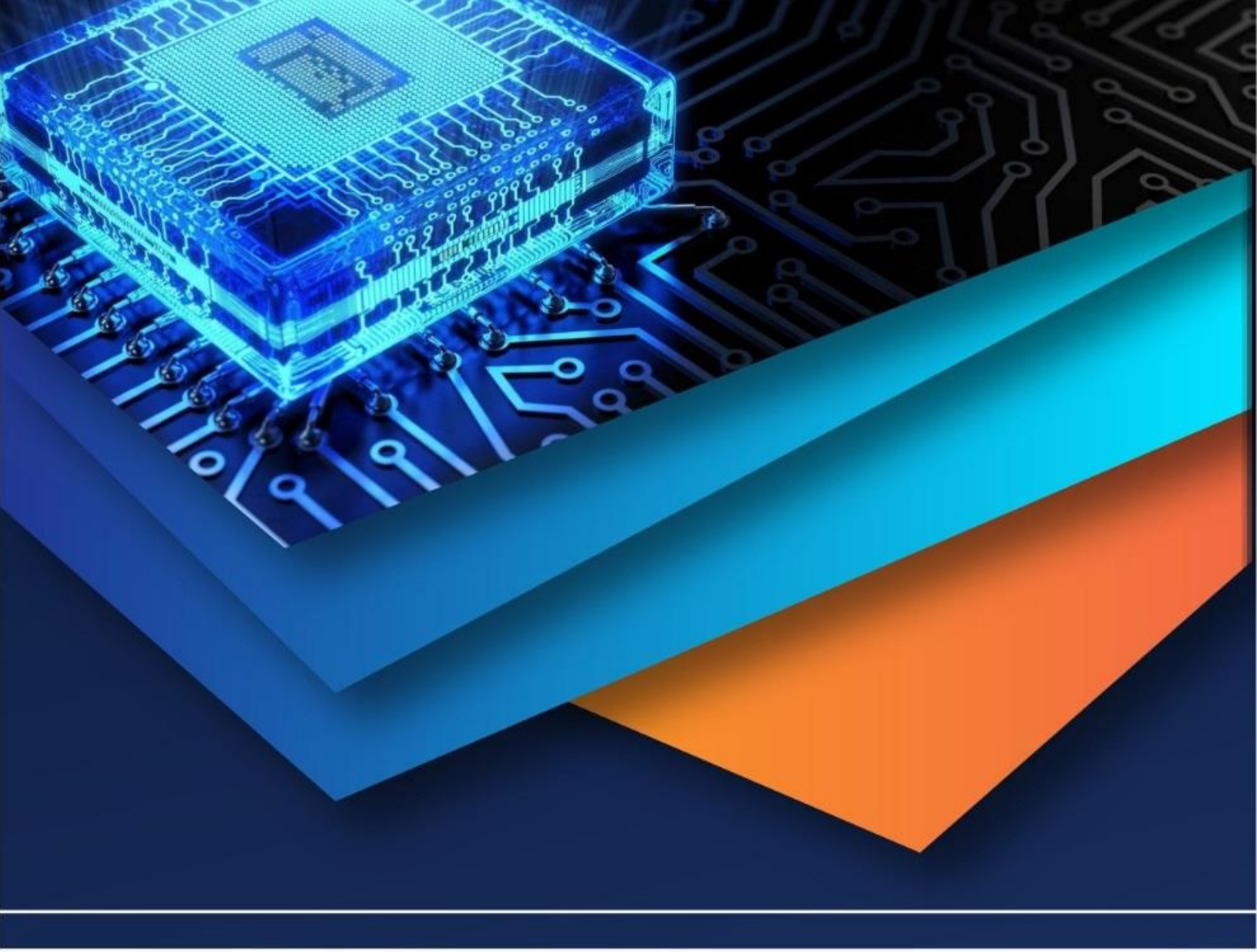
V. CONCLUSION

Blockchain-based electronic voting applications have been suggested in scientific literature, but few have been put into practice and none have undergone extensive testing. While the blockchain's underlying concepts are secure, e-voting apps are still susceptible to a number of attacks, making it difficult to ensure the validity of an election. Moreover, Blockchain does not eliminate the requirement for a central authority to oversee elections because the mere act of organizing a national election entails some degree of centralization. However, blockchain can be used as an addition to existing systems, such as counting paper ballots at the level of each municipality or region using a blockchain would lessen the possibility of fraud and lack of confidence.

In nations with sizable populations, blockchain-based voting apps for smartphones (in addition to traditional polling places) will enable a greater involvement of those who were previously cut off from the political process due to their remote location. However, It is significant to remember that internet voting, including blockchain-based voting apps are not and will not be a secure voting method in the United States in the near future, according to research from NASEM (National Academies of Science, Engineering, and Medicine) and other organizations.

REFERENCES

[1] Farooq. A Framework to Make Voting System Transparent Using Blockchain Technology. IEEE Access. 2022.
[2] Anıl L, Sertkaya I. "Requirement Analysis of Some Blockchain-based E-voting Schemes" [Internet] 2023.
[3] K M, A framework to make charity collection transparent and auditable using blockchain technology. 2020.
[4] Ramesh S. E-Voting Based on Block chain Technology [Internet], IJEAT, 2019.
[5] Lunesu MI, Pani FE, Pinna A. Crypto-voting, a blockchain based e-voting system. IC3K 2018 SciTePress.
[6] Chung KS. Design of Blockchain based e-Voting System for Vote Requirements. J Phys. 2021
[7] Krimmer R, "New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?" 2021.
[8] Rivest RL, "Going from bad to worse: From Internet voting to blockchain voting", Cybersecur. 2021;
[9] Bertin E, "A decision tree for building IT applications: What to choose: blockchain or classical systems?" Telecommunications. 2021
[10] Dimitriou T, "Coercion-free and Universally Verifiable Blockchain-based Voting", CN. 2020
[11] KM, investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems. 2020
[12] Javed S F, "The Future of Electronic Voting System Using Blockchain". [Internet]. 2020
[13] Bana G. Time, Privacy, Robustness, Accuracy: Trade Offs for the Open Vote Network Protocol 2022.
[14] Youssef AM. Dispute-free Scalable Open Vote Network using zk-SNARKs. 2022
[15] Gaikwad AT, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology". ICSIDEMPC 2020
[16] Che Z. Security and privacy in smart city: a secure e-voting system based on blockchain. IJECE 2023.
[17] Caro, Transparent voting system using blockchain. Sensors. 2023
[18] Se S, An Efficient Open Vote Network for Multiple Candidates. IEEE Access. 2022.
[19] Li T. D-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. IEEE. 2021.
[20] Tore E. On Secure E-Voting over Blockchain. Digital Threats. 2021.
[21] Bag S. "A Smart Contract System for Decentralized Borda Count Voting". IEEE 2020.
[22] Sha S. Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach. IEEE. 2023.
[23] Li H. A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era. IEEE. 2021.
[24] Iqbal R. On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities. IEEE. 2022.
[25] Dara O. Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections. Informatics. 2020.
[26] Khan M. Simulation of transaction malleability attack for blockchain-based e-Voting. Computers 2020
[27] Paw M. Trends in blockchain-based electronic voting systems. IPM. 2021.
[28] Hu C. An anti-quantum e-voting protocol in blockchain with audit function. IEEE. 2019.
[29] Ye K. A Coercion-Resistant E-Voting System Based on Blockchain Technology. IJNS. 2021
[30] Hao F. End-to-end Verifiable E-voting Trial for Polling Station Voting, IEEE 2022
[31] Ren J. Bitcoin and Blockchain: Security and Privacy. IEEE. 2020.
[32] Rifa H. SeVEP: Secure and Verifiable Electronic Polling System. IEEE. 2019.
[33] de R. PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. Future Internet. 2023 Apr 1;15(4).
[34] Xu B, Ques-Chain: an Ethereum Based E-Voting System. 2019 May 13.
[35] Wan Z, PriScore: Blockchain-Based Self-Tallying Election System Supporting Score Voting. IEEE 2021.
[36] Li Y, ACB-Vote: Efficient, Flexible, and Privacy- Preserving Blockchain-Based Score Voting with Anonymously Convertible Ballots. IEEE 2023.
[37] Luo, A Blockchain-Based Self-Tallying Voting Protocol with Maximum Voter Privacy. IEEE. 2022;
[38] Boko N. An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions, IEEE.2022.
[39] Shin JS. A New Distributed, Decentralized Privacy-Preserving ID Registration System. IEEE. 2021
[40] N Lu. Large-scale Election Based on Blockchain. Elsevier; 2018.
[41] Kota D. An anonymous distributed electronic voting system using Zerocoin [Internet].
[42] Bara A, Andreescu AI, Cristescu MP. Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level. IEEE. 2023.
[43] Ta R. A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. Communications; 2021.
[44] Crow C. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE. 2019.
[45] Hu J. A Survey PPBS and a Novel PPBS-Based Framework for Smart Agriculture. IEEE. 2021.
[46] Zan F, Blockchain Technology as a Framework Blockchain Technology: A Framework for Endless Applications. 2022.
[47] J Li. MAS-Encryption & its Applications in Privacy-Preserving Classifiers. IEEE 2022.
[48] Pawla M. Towards the intelligent agents for blockchain e-voting system. Elsevier 2018.
[49] Ro CH. A study on electronic voting system using private blockchain. JIPS. 2020.
[50] Yan T. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI. 202



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY