iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51892

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 V May 2023- Available at www.ijraset.com

Online Voting System Using Blockchain Technology

Divya Khude[1], Revati Dhawale[2], Shreya Kadam[3], Sayali Rankhamb[4], Ms. Shwetkranti Taware[5]
Indira College of Engineering & Management, Pune.

Abstract: ***An online voting system that utilizes blockchain technology is a promising solution for conducting elections in a secure and transparent manner. The decentralized and distributed nature of the blockchain ledger ensures that every vote is recorded accurately and cannot be tampered with or altered without detection. This is because every node on the blockchain network has a copy of the ledger, making it virtually impossible to manipulate election results. One of the biggest advantages of blockchain-based voting systems is that they allow voters to cast their ballots from anywhere, as long as they have an internet connection. This makes voting more accessible and convenient for people who might have difficulty getting to a polling station. Additionally, blockchain technology allows for the verification of voter identity and prevents double voting, ensuring that every vote is legitimate and counted accurately. Another benefit of blockchain-based voting systems is their resistance to cyber attacks. The decentralized nature of the blockchain network makes it extremely difficult for hackers to compromise the system, as they would need to gain control of a majority of the nodes on the network. Additionally, the transparent nature of blockchain-based voting systems makes them more trustworthy and helps to prevent voter fraud.***

Overall, the use of blockchain technology in online voting systems has the potential to revolutionize the way we conduct elections and safeguard the integrity of democracy. By providing a secure and transparent method for conducting elections, blockchain-based voting systems can help to increase voter participation and ensure that every vote is counted accurately.

Keywords: online voting system, blockchain technology, secure, transparent, double voting prevention, cyber attack resistance, voter identity verification.

I. INTRODUCTION

The traditional method of conducting elections has been through in-person voting at a polling station. However, as society becomes increasingly digital, the need for a more accessible and convenient method of voting has emerged. Online voting has been proposed as a solution to this problem, but concerns surrounding security and transparency have hindered its widespread adoption. Enter blockchain technology, a decentralized and distributed ledger system that provides a secure and transparent method for recording transactions. With its built-in security features, blockchain technology has the potential to provide a tamper-proof system for online voting, ensuring that every vote is counted accurately and that the results of an election are trustworthy.

Blockchain-based online voting systems work by recording each vote on a decentralized ledger that is accessible to all nodes on the network. Each vote is encrypted and signed using a private key, ensuring that it cannot be tampered with or altered without detection. This provides a level of security that traditional voting systems cannot match, as there is no central point of failure that can be exploited by hackers. One of the biggest advantages of blockchain-based online voting systems is their accessibility. Voters can cast their ballots remotely, from anywhere with an internet connection. This makes voting more convenient for people who might have difficulty getting to a polling station, such as those with disabilities or those who live in remote areas.

Another benefit of blockchain-based online voting systems is their ability to verify voter identity and prevent double voting. By using a combination of encryption and digital signatures, blockchain technology can ensure that every voter is who they claim to be and that they can only cast one vote.

II. LITERATURE REVIEW

Issues and Effectiveness of Blockchain Technology on Digital Voting: System presented in the Issues and Effectiveness of Blockchain Technology on Digital Voting that block chain is a technology that enables moving digital coins or assets from one individual to other individual. Blockchain concept can be understand with the concept of linked list in Data Structure, because its next key address are stored in previous key and they are linked with each other. [1]

Electronic voting machine based on Blockchain technology and Aadhar verification: System presented in the Electronic voting machine based on Blockchain technology and Aadhar verification that A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy election amongst the people of the democracy. Since aadhar card is the most needed for a person identity hence deploying an election process using it is highly recommendable. Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it.[2]

E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy: E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy that a potential solutionto the lack of interest in voting amongst the young tech savvypopulation. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on block chain technology. This paper explores the potential of the block chain technology and its usefulness in the e-voting scheme. an e-voting scheme, which is then implemented. [3]

Design of Distributed Voting Systems: System **p**resent the Design of Distributed Voting Systems. Electronic voting systems attempt to be as easy to use and secure as ideal traditional elections and attempt to eliminate the human errors described. [4]

A secure end-to-end verifiable e-voting system using zero knowledge based blockchain: System presented in the secure end-to-end verifiable e-voting system using zero knowledge based blockchain that present a cryptographic technique for an authenticated, end-to-end verifiable and secret ballot election. Voters should receive assurance that their vote is cast as intended, recorded as cast and tallied as recorded. The election system as a whole should ensure that voter coercion is unlikely, even when voters are willing to be influenced. Currently, almost all verifiable e-voting systems require trusted authorities to perform the tallying process. An exception is the DRE-i and DRE-ip system. The DRE-ip system removes the requirement of tallying authorities by encrypting ballot in such a way that the election tally can be publicly verified without decrypting cast ballots. However, the DRE-ip system necessitates a secure bulletin board (BB) for storing the encrypted ballot as without it the integrity of the system may be lost and the result can be compromised without detection during the audit phase.[5]

III. REQUIREMENTS

A. H/W Requirements

1) System : i5 2.7 GHz.
2) Hard Disk : 300 GB
3) Monitor : 15 VGA Color.
4) Mouse : Logitech.
5) Ram : 4 GB

B. S/W Requirements

1) Operating system: Windows XP/7 Higher
2) Programming Language: JAVA/J2EE/
3) Tools: Eclipse, Heidi SQL, JDK 1.7 or Higher
4) Database: MySQL 5.1

C. Proposed Algorithm/Methodology

Algorithm 1 : Hash Generation
Input : Genesis block, Previous hash, data d,
Output : Generated hash H according to given data
Step 1 : Input data as d
Step 2 : Apply SHA 256 from SHA family
Step 3 : CurrentHash= SHA256(d)
Step 4 : Return CurrentHash

This algorithm outlines the steps needed to generate a hash using SHA-256 from the SHA family. The input includes a genesis block, a previous hash, and the data d, while the output is the generated hash H according to the given data.

In Step 1, the data is input as d. This can be any type of data, such as a transaction or a block header.

In Step 2, the SHA-256 algorithm is applied to the input data. This is a cryptographic hash function that creates a fixed-length output, known as a hash, from any input data.

In Step 3, the output of the SHA-256 algorithm is stored as the current hash, represented by the variable CurrentHash.
Finally, in Step 4, the algorithm returns the CurrentHash as the generated hash H according to the given data.
This algorithm is a crucial component of blockchain technology, as it helps to ensure the integrity of the data stored on the blockchain. By using a cryptographic hash function like SHA-256, each block on the blockchain is linked to the previous block in a tamper-proof way. Any attempt to modify the data in a block would result in a different hash, breaking the link to the chain and alerting the network to the attempted tampering.

Algorithm 2 : Protocol for Peer Verification

Input : User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain],

Output : Recover if any chain is invalid else execute current query

Step 1 **:** User generate the any transaction DDL, DML or DCL query

Step 2 : Get current server blockchain

Cchain ← Cnode[Chain]

Step 3 : For each

$$NodesChain\,[Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End for

Step 4 **:** Foreach (read I into NodeChain)

If (!.equals NodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

Step 5 **:** if (Flag == 1)

Count = SimilaryNodesBlockchian()

Step 6 **:** Cacluate the majority of server

Recover invalid blockchin from specific node

Step 7**:** End if

End for

End for

This algorithm outlines the steps needed to verify the integrity of a blockchain by checking it against other nodes in a peer-to-peer network. The input includes a user transaction query, the current node chain CNode[chain], and the remaining nodes in the blockchain NodesChain[Nodeid][chain]. The output is either to recover if any chain is invalid, or else execute the current query.
In Step 1, the user generates a transaction query, which can be a DDL, DML, or DCL query.
In Step 2, the current server blockchain is obtained by assigning it to the variable Cchain, which is equal to CNode[chain]. This ensures that the current node is using the correct blockchain.
In Step 3, a loop is initiated to iterate over all the nodes in the network.
In Step 4, another loop is initiated to read each node's blockchain, represented by the variable NodeChain[i]. If the NodeChain[i] is not equal to Cchain, then Flag is set to 1, indicating that there is an invalid blockchain in the network. Otherwise, the algorithm continues to commit the query.
In Step 5, if Flag is equal to 1, then the algorithm proceeds to calculate the majority of the servers that have the same blockchain, represented by the variable Count.
In Step 6, once the majority of servers with the same blockchain is computed, the algorithm recovers the invalid blockchain from a specific node.
Finally, in Step 7, the algorithm ends the loop and continues to execute the query.
This algorithm is critical for maintaining the integrity of the blockchain and preventing fraudulent activities, such as double-spending and tampering with transaction records. By verifying the blockchain with other nodes in the network, the algorithm ensures that the blockchain is valid and that the transactions are secure.

Mining Algorithm for valid hash creation
Input : Hash Validation Policy P[], Current Hash Values hash_Val
Output : Valid hash
Step 1 **:** System generate the hash_Val for ith transaction using Algorithm 1
Step 2 **:** if (hash_Val.valid with P[])
Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3 **:** Return valid hash when flag=1

This algorithm outlines the steps needed to mine a valid hash for a given transaction. The input includes the Hash Validation Policy P[] and the current hash values hash_Val, and the output is a valid hash.

In Step 1, the system generates the hash value for the ith transaction using Algorithm 1. This hash value is represented by the variable hash_Val.

In Step 2, the algorithm checks if the hash_Val is valid with the Hash Validation Policy P[]. If the hash_Val is valid, then the algorithm returns the valid hash and sets the flag to 1. Otherwise, if the hash_Val is not valid, the algorithm sets the flag to 0 and mines again randomly until a valid hash is found.

In Step 3, once the flag is set to 1, the algorithm returns the valid hash.

The mining algorithm is used in blockchain technology to create new blocks in the chain. In order to add a new block to the chain, miners must solve a complex mathematical problem that involves finding a hash value that meets a certain criteria, as defined by the Hash Validation Policy. This algorithm is responsible for generating a valid hash value based on the given policy and current hash values.

The mining process is computationally intensive, which ensures the security of the blockchain. Miners compete with each other to solve the problem, and the first one to find a valid hash is rewarded with newly generated cryptocurrency and transaction fees. The mining algorithm is a crucial component of the blockchain, as it ensures the integrity of the transactions and the security of the network.

IV. FIGURES

A. System Architecture

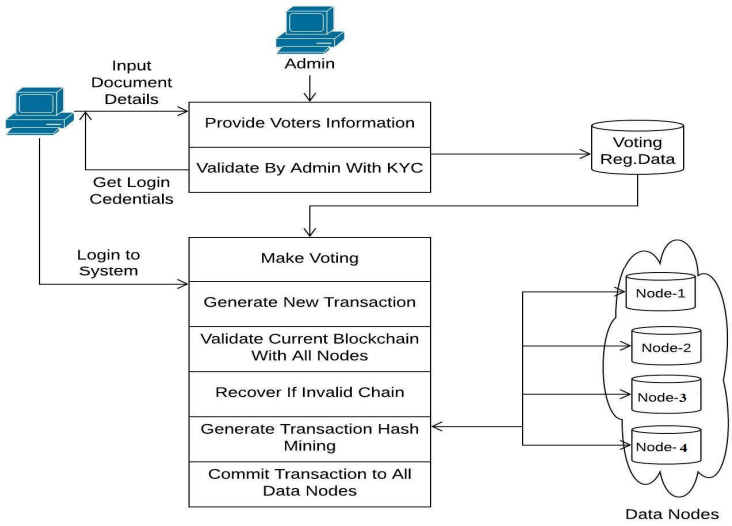


Fig.4.1. System Architecture

This system highlights the implementation of e-voting using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding this work is a potential roadmap for blockchain technology to be able to support complex applications. Building an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies is an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems.

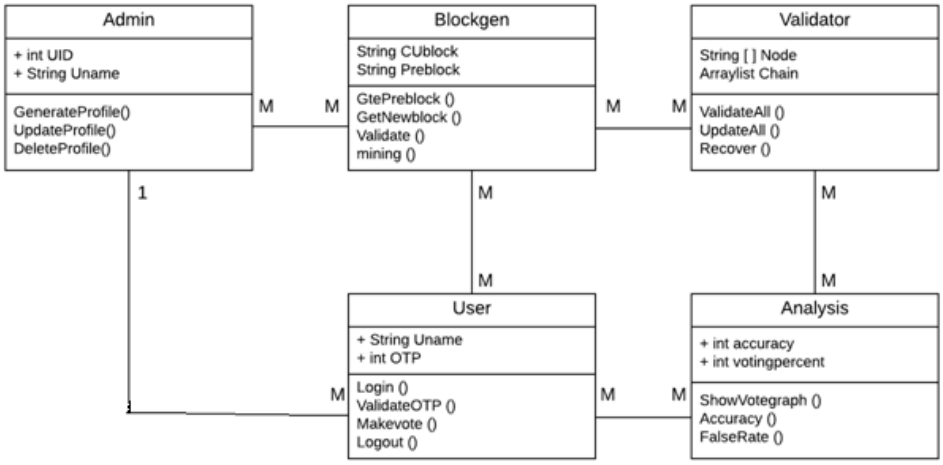


Fig.4.2 Class Diagram

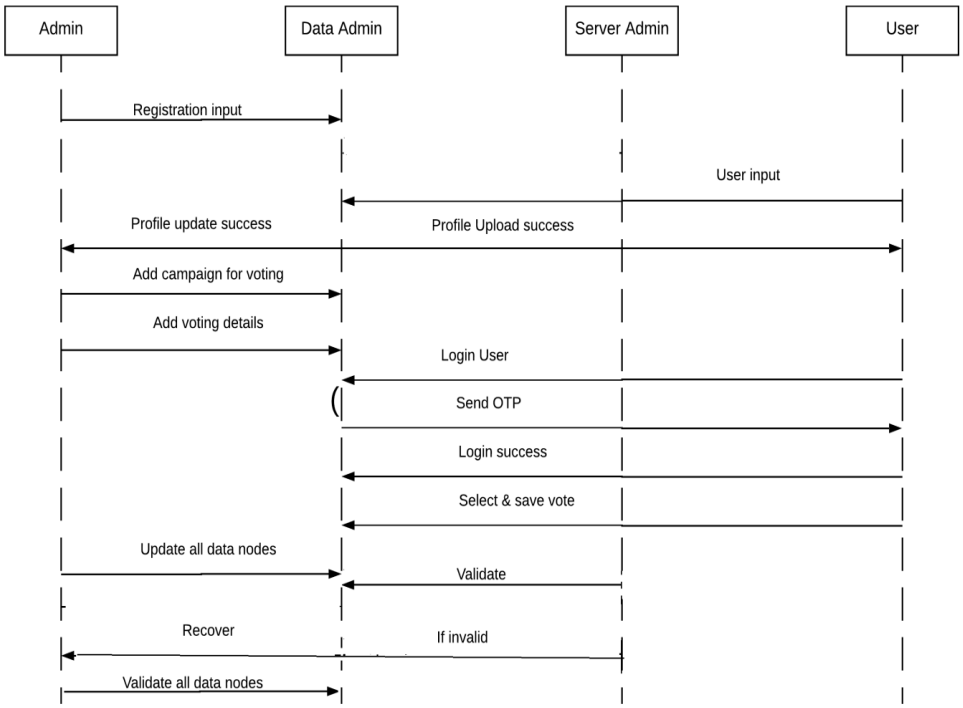


Fig.4.3 Sequence Diagram

V. SPECIFICATIONS

A. Applications

1) Political elections: The most obvious application of blockchain-based online voting systems is in political elections. By providing a secure and transparent method for recording votes, these systems can help to increase voter participation and ensure that every vote is counted accurately.
2) Corporate elections: Many corporations hold elections for their Board of Directors or other leadership positions. Blockchain-based online voting systems can provide a secure and transparent method for recording votes in these elections, ensuring that the results are trustworthy.
3) Union elections: Labour unions often hold elections for their leadership positions or to make decisions that affect their members. Blockchain-based online voting systems can provide a secure and transparent method for recording votes in these elections, ensuring that the results are trustworthy.
4) Non-profit organization elections: Non-profit organizations often hold elections for their Board of Directors or other leadership positions.

B. Advantages

1) Increased security: Blockchain technology provides a secure and tamper-proof method for recording votes. This makes it virtually impossible for anyone to manipulate or alter the results of an election.
2) Transparency: Blockchain-based online voting systems provide complete transparency, allowing voters to track their votes and ensuring that the election results are accurate.
3) Increased voter participation: Online voting systems are convenient and accessible, which can help to increase voter participation. Voters can cast their votes from anywhere in the world, at any time, without having to physically go to a polling station.
4) Cost-effective: Online voting systems are generally more cost-effective than traditional paper-based voting systems. They require less manpower to administer and can be conducted more quickly and efficiently.
5) Faster results: Blockchain-based online voting systems can provide faster results than traditional paper-based voting systems. This is because the votes are recorded and counted in real-time, eliminating the need for a manual vote-counting process.
6) Reduced fraud: Online voting systems using blockchain technology can help to reduce fraud and ensure that every vote is counted accurately. This is because the system is designed to prevent double voting and other forms of fraudulent activity.

C. Future Scope

The future scope of online voting systems using blockchain technology is immense. Here are some potential developments that we might see in the near future:

1) Increased Security: One of the main advantages of blockchain technology is that it is highly secure and tamper-proof. This means that online voting systems using blockchain can ensure the integrity of the voting process, preventing any kind of fraud or manipulation.
2) Increased Transparency: Blockchain technology also allows for increased transparency in the voting process. This means that voters can have greater confidence in the electoral process, knowing that their votes are being counted accurately and fairly.
3) Greater Accessibility: Online voting systems using blockchain can also increase accessibility, particularly for people who might have difficulty accessing traditional polling places. This can include people with disabilities, people who live in remote areas, or people who are unable to take time off work to vote.
4) Improved Efficiency: Blockchain technology can also improve the efficiency of the voting process, reducing the time and resources required to administer an election. This can help to increase voter turnout and reduce the costs associated with running an election.
5) Decentralization: Finally, blockchain technology allows for decentralization, meaning that there is no central authority controlling the voting process. This can help to increase trust in the electoral process and reduce the risk of corruption or manipulation.
6) Overall, the future of online voting systems using blockchain technology is bright, with the potential to revolutionize the way we conduct elections and increase the transparency and integrity of the democratic process.

VI. CONCLUSION

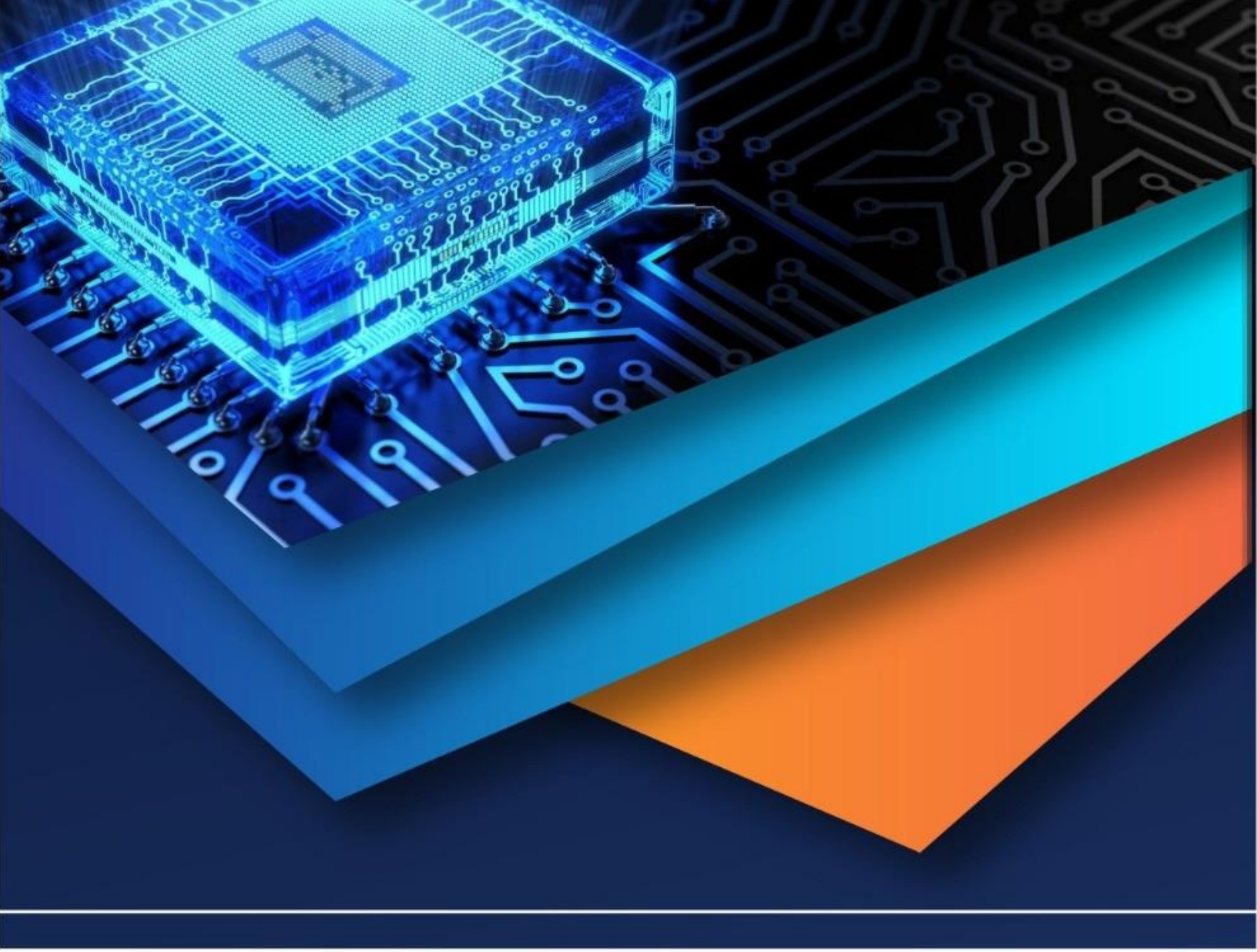
In conclusion, the integration of blockchain technology into online voting systems has the potential to transform the way we conduct elections. The use of blockchain can provide a secure and tamper-proof system that ensures the integrity of the voting process, while also increasing transparency, accessibility, and efficiency. With the decentralization of the voting process, voters can have greater confidence in the electoral process and reduce the risk of corruption or manipulation. While there are still challenges to overcome, such as ensuring privacy and addressing technical issues, the future of online voting systems using blockchain technology looks promising and could lead to a more trustworthy and democratic voting process.

VI. ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have supported me in the completion of this research paper. First and foremost, I would like to thank my mentor Ms. Shwetkranti Taware for their constant guidance and encouragement throughout the research process. Their insights and suggestions have been invaluable in shaping the direction of my research.
I am also grateful for their contributions to this research. Their expertise and input have been instrumental in achieving the research objectives, and their involvement has been greatly appreciated. I would like to extend my thanks to the participants who took part in this research and shared their insights and experiences. Without their willingness to participate, this research would not have been possible.Finally, I would like to thank everyone who has contributed to the success of this research paper. Your support and guidance have been greatly appreciated.

REFERENCES

[1] Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1
[2] Navya A., Roopini R., SaiNiranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)
[3] Hardwick, Freya Sheer, Raja NaeemAkram, and Konstantinos Markantonakis. "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy." arXiv preprint arXiv:1805.10258 (2018).
[4] Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017).
[5] Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."
[6] Martin A Makary and Michael Daniel. Medical error-the third leading cause of death in the us. BMJ: British Medical Journal (Online), 353, 2016
[7] Paul Tak Shing Liu. Medical record system using blockchain, big data and tokenization. In International Conference on Information and Communications Security, pages 254–261. Springer, 2016.
[8] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, pages 1–10. IEEE, 2013.
[9] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences, pages 358–367. IEEE, 2016.
[10] Dongsheng Zhang. Resilience enhancement of container-based cloud load balancing service. Technical report, PeerJ Preprints, 2018.
[11] Dongsheng Zhang. Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks. PhD thesis, University of Kansas, 2015.
[12] Dongsheng Zhang and James P.G. Sterbenz. Modelling critical node attacks in MANETs. In Self-Organizing Systems, volume 8221 of Lecture Notes in Computer Science, pages 127–138. Springer Berlin Heidelberg, 2014.
[13] Dongsheng Zhang and James P. G. Sterbenz. Analysis of Critical Node Attacks in Mobile Ad Hoc Networks. In Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 171–178, Barcelona, Spain, November 2014.
[14] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. Modelling Wireless Challenges. In Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom), pages 423–425, Istanbul, August 2012. Extended Abstract.
[15] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. Modelling Attacks and Challenges to Wireless Networks. In Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 806–812, St. Petersburg, October 2012.
[16] Dongsheng Zhang and James P. G. Sterbenz. Measuring the Resilience of Mobile Ad Hoc Networks with Human Walk Patterns. In Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, October 2015.
[17] Dongsheng Zhang and James PG Sterbenz. Robustness Analysis and Enhancement of MANETs using Human Mobility Traces. Journal of network and systems management, 24(3):653–680, 2016.
[18] Dongsheng Zhang and James P. G. Sterbenz. Robustness analysis of mobile ad hoc networks using human mobility traces. In Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN), Kansas City, USA, March 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY