iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48810

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 I Jan 2023- Available at www.ijraset.com

Survey on Secured Digital Voting System using Blockchain Technology

Bhagya A Koushik[1], Deekshitha R S[2], Gowthami S[3], Haritha Nandhini[4], Dr. Nagaraja J[5]
Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore

Abstract: ***Blockchain is a shared tamper-proof ledger that eases the process of recording transactions and tracking assets in a business network. Traditional voting system has various disadvantages with respect to its security, fairness and integrity. Digital voting is a form of computer driven voting in which voters can cast their votes on a system over the internet. This paper uses blockchain to serve this purpose. It employs a decentralized blockchain network to monitor the entire election process. SHA- 256 algorithm is used to ensure encryption of the votes and avoid any kind of manifestation of votes during the election. It generates a user- friendly election environment over the internet to allow the users to cast their votes to their candidates of interest and also announces the final results giving information about the winner and also the election statistics.***
Keywords: Blockchain, Ganache, Hashing, Meta-mask, Smart contract, Truffle, Voting system.

I. INTRODUCTION

In the democratic world, one of the fundamental rights of citizens is to cast a vote to choose their leaders. For many years, paper ballots were used to cast votes during elections all around the world. But this process is extremely time and resource consuming. It was one of the major electoral frauds registered. Currently Electronic Voting Machines is an alternative to the traditional paper ballots and have brought about consistent changes in the voting system. Although this approach is more advantageous, it still lacks in many ways in terms of integrity of votes. With the current advancements in technologies, there is also rise in cyber-crimes which include hacking of EVM's to alter the results of the election. The lack of transparency is the major loop hole in the overall process of election which leads to tampering of votes by influencing the polling staff and thereby generating a biased result. Sometimes, there can be unsupervised vote counting and lack of audits and appeals which can prove to be disadvantageous.

Blockchain uses peer-to-peer networking which brings in transparency. It is a distributed ledger which uses the SHA-256 algorithm for encryption. Also, the votes casted will be hashed and recorded in blocks. This makes the system immutable and the votes cannot be tampered. All of these features of blockchain helps to reduce the disadvantages in the current system which is one of the reasons for people to be shifting towards blockchain based digital voting system in the present day.

II. LITERATURE SURVEY

Somnath Panja et al., [1] proposed A Secure end-to-end verifiable e-voting system using blockchain and cloud server which gives a cryptographic solution to create an authenticated, end-to-end verifiable secret ballot election. It brings up the disadvantages of the DRE-ip system and suggests a new solution to maintain the voter registration and authentication mechanism by preventing the ballot stuffing attack. It publishes the final tally without specifying the tally from DirectRecording Electronic (DRE) machines with multiparty computation. It has brought forward the new and improved NIZK proof which lifts up the overall efficiency of the system. The protocol has the potential for real-world deployment. The model failed to propose the scheme to decrease the False Rejection Rate of the Fussy Vault algorithm with respect to fingerprint.

Jen-Ho Hsiao et al., [2] proposed Decentralized EVoting Systems Based on the Blockchain Technology which combines the pros and properties of Pailler's homomorphic encryption, oblivious transfer and secret sharing scheme to construct a decentralized electronic voting system. The Pailler's public-key cryptosystem with secret sharing scheme helps to achieve anonymity and security. The major advantage is transparency of smart contract that allow voters to record and verify ballots. This system boosts the votes' confidence and decreases the election resources wastage.

Kibin Lee et al., [3] proposed Electronic Voting Service Using Block-Chain which focuses on the advantages of blockchain over encrypted transactions. SHA 256 and RIPEMD160 is used to generate public key hash which is of 160 bits and it is Base58Check encoded to produce Bitcoin address. In this paper, consensus attack will not be able to steal coins, consume coins or change ownership records and past transactions. The limitation in this model is that it is susceptible to denial-of-service attacks that can affect the formation of blocks since blockchain network has considerable hashing power.

©IJRASET: All Rights are Reserved

Ashish Singh et al., [4] proposed SecEVS : Secure Electronic Voting System Using Blockchain Technology which provides an online electoral process on blockchain and employs transparency, decentralization, irreversibility and non- repudiation. It is secured with the powerful SHA-256 algorithm. The framework makes use of Zone Blockchain to ensure secured and untampered election process in each zone of a university. This model allows the voter to register himself only once. This is followed by the voting process where encryption of the vote is done to prevent any tampering with the vote during the counting process and it can be verified using the public key. Each voting transaction requires 84 bytes of memory space. Hence, it is difficult to implement on large scale.

Syada Tasmia Alvi et al., [5] proposed Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract which uses Merkle tree and fingerprint has to authenticate voters. The major objective is to design a online electoral system which includes smart contract to overcome the challenges which crop up during blockchain adaption along with voting and provide mobility, transparency and integrity. Scalability will be achieved since the voters' information will be hashed and recorded in blockchain. Miners are employed by smart contracts to improve the overall speed of transactions. In this model, the limitation is that the vote counting is not done immediately which increases the consumption of time and decreases the number of voters. There is no encryption technique to boost the system's security.

Harsha V Patil et al., [6] proposed IRJET – A Study on Decentralized E-Voting System Using Blockchain Technology which allows the voters to register only with the confirmation number that will be provided to them by the concerned authorities. It ensures that no fake identities can be created to attack the model and avoids the occurrence of Sybil attack in future. This model provides the voters with an option to cast a protest vote in case they are not satisfied with the current elections or candidature. SHA one-way hash function which is uni-directional is used to encrypt each and every vote. Technically, the only possible way to retrieve the information is by choosing the seed data, the algorithm used. This has to be hashed to see if the results are going to match. The limitations of the EVoting system proposed in this model is that more energy is required to validate and process the votes, there will be a shift from the central election commission and building the trust factor is also a challenge.

Abhishek Kaudare et al., [7] proposed Implementing Electronic Voting System With Blockchain Technology which compares the various existing blockchain technologies to improve the Voting system. Decentralized approach along with a Secured ecosystem is used for the sake of security of the system. Consensus algorithm is used as the base architecture in this model. Distributed Ledger Technology is used to record and retrieve all the data involved in this model. Since Blockchains are strongly associated with linked lists, every block has a data store that maintains the data regarding a transaction and also previous block is linked on to the same. When compared to Ethereum, Hyperledger is observed to be more efficient taking the performance metrics into consideration. Also, the permissioned blockchain allows the model to maintain the privacy of the voter by not revealing his credentials.

Md. Razu Ahmed et al., [8] proposed The Future Of Electronic Voting System Using Blockchain which represents secured decentralized database of voter information and casted vote which deposited against private key and digital signature. It has main parameters as authentication, verifiability, anonymity, accuracy and it overcomes the problem when more than one user cast their vote at the same time which will be connected to hash in the previous block using Longest Chain Rule. The blocks created are identified by the SHA-256 generated hash value. The limitation in this framework is that the vote casting machine is susceptible to malicious attackers who install vicious software into the device. Voters can cast their vote only once and it cannot be withdrawn.

Kriti Patidar et al., [9] proposed Decentralized EVoting Portal Using Blockchain provides a model which is suitable for small scale elections that are held within an organization, or a committee. It uses Truffle framework for the development, validation and deployment of the Ethereum smart contracts. Smart contract deployment requires migrations to update the network. For every smart contract, a migration has to be created with a numbered java script file. Meta-mask works as wallet and Ganache is the software to test the client. It uses permissionless public blockchain network so that the database can be checked by the public for any manipulations. The users and candidates have their individual accounts which are secured with RSA algorithms. The limitations of this model are that the voting system needs to be supplied by continuous broadband access and the users require digital skills. Implementation of this model on large scale requires more analysis.

Kashif Mehboob Khan et al., [10] proposed Secure Digital Voting System Based on Blockchain Technology which focuses on to examine the key problems such as end-to-end verification, voter anonymity and confidentiality. Multichain is the technology used to develop the system and a strong cryptographic hash is obtained for each vote transaction to protect security and privacy of vote. The limitation of this system is that it does not check for double spending problem which will lead to double voting.

Haibo Yi [11] proposed Securing e-voting based on blockchain in P2P network which provides the voter credentials model i.e., the authentication of the users is done on the basis of Elliptic Curve Cryptography (ECC) model. This model provides the users with an option to modify their vote before the specified time.

When two blocks having same timestamp is to be added to the blockchain, the block which has the highest signature value is selected. Public blockchain is used and hash value of the votes requires the private key signature which is done using the ECDSA signature. The use of ECC model is advantageous but is also susceptible to quantum computer attacks.

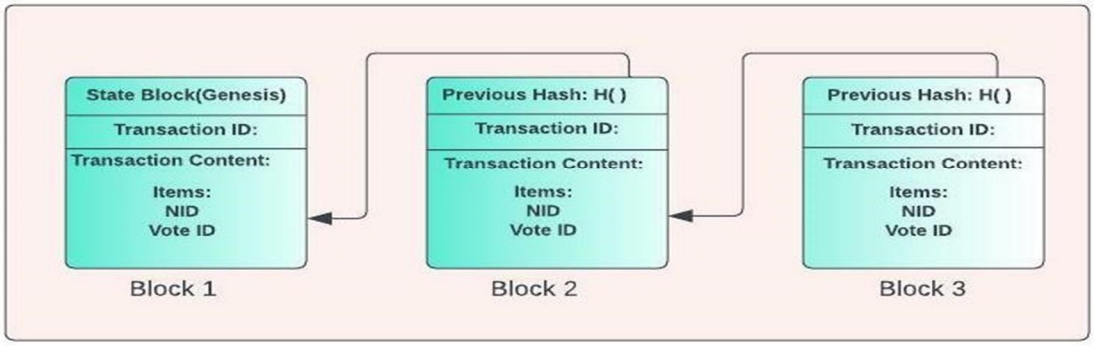
Ketulkumar Govindbhai Chaudhari [12] proposed Evoting system using Proof of Voting (POV) consensus algorithm using Block chain Technology which uses consensus Proof-Of-Voting (POV) algorithm which increases security, low power consumption and cost. Digital electoral process utilizes the smart contract to provides guaranteed voters' privacy. The malicious nodes are predicted using Proof-Of-Voting (POV) and removed from blockchain using consensus algorithm. This algorithm also removes some failures like security failure, temporal failure, byzantine failure. This system is centralized and the network-type is distributed. So, the disadvantage is that the network is more susceptible to single point of failure.

Camilo Denis Gonzalez et al., [13] proposed Electronic Voting System Using an Enterprise Blockchain which provides another approach for participatory management processes like e-voting, focused on trust, transparency, and immutability. The Hyperledger Fabric framework is used to represent the proof of concept that can be modified to different electing scenario. This research is proposed to decrease the vote-counting time and provides high traceability capacity without high energy utilization compared to other blockchain technologies and allows the validators to monitor the election procedure without violating privacy. This paper can verify validity of vote, avoid double-counting, guarantee the vote are casted from an authorized device but cannot guarantee the device from which vote has been casted is free of malicious software. The voting in blockchain is similar to Direct recording electronic voting machine due to the easy to use and ability to efficiently case vote. But recently DREs are frequently attacked by cybersecurity experts. Some of these security issues has to be prevented.

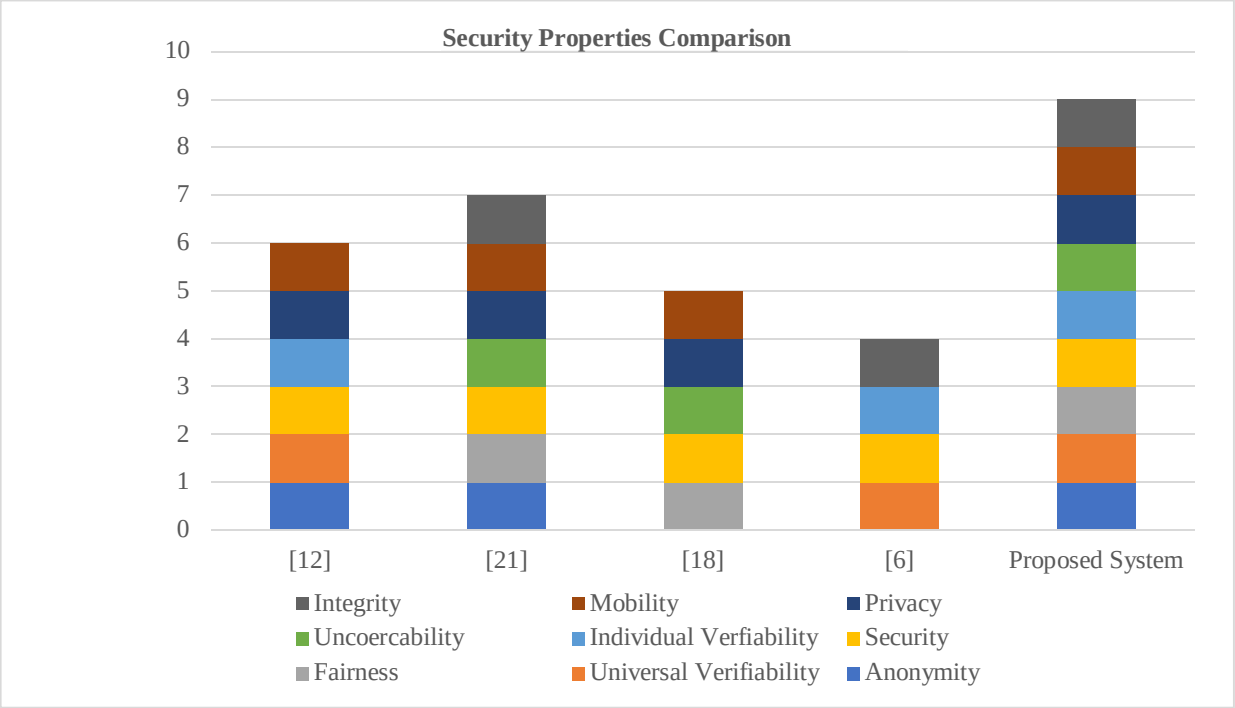
Xuechao Yang et al., [14] proposed Decentralized Voting: A Self-tallying Voting System Using a Smart Contract on the Ethereum Blockchain which concentrates on blockchain based digital voting makes use of smart contract and cryptographic techniques. The existing voting proposals uses public bulletin to store vote data but, in this paper, self-tallying voting system deployed on Ethereum is used which reduces the burden on election authorities. Score voting helps voters to allocate points to various candidates without any restriction. This system may suffer abortive issue. There is an assumption that all voters have submitted their votes else, any voter can end the tally without casting their vote. In order to perform trials at a larger scale the model is migrated to an Ethereum network.

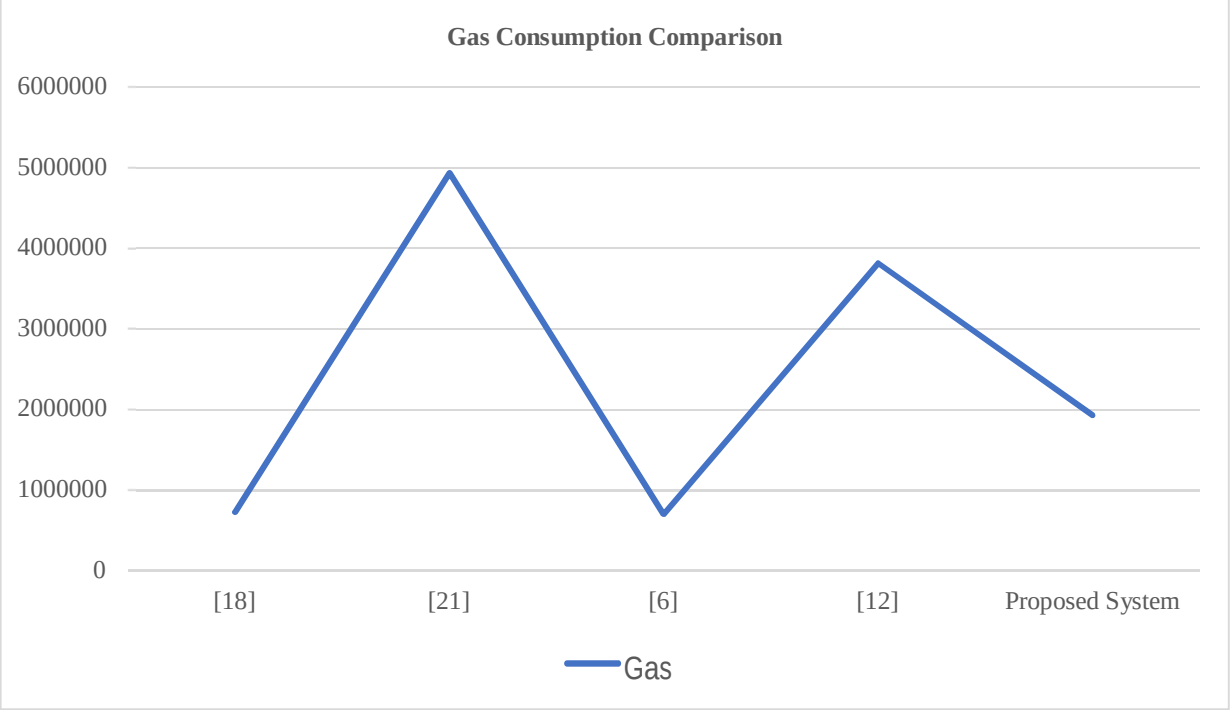
Basit Shahzad et al., [15] proposed Trustworthy Electronic Voting Using Adjusted Blockchain Technology which introduces a framework which uses effective hashing techniques to ensure data security. Creation and sealing of blocks is introduced to ensure that the blockchain to meets the requirements of the polling process. Consortium Blockchain is used since it has better mining speed when compared to the private blockchain. Voter authentication is done using hash function generated through MD5 algorithm. This voting process allows the voters to cast multiple votes but only the latest vote is considered and rest of them are cancelled. This is followed by the result phase which displays the votes obtained by each candidate and also the final result of the election. This framework assumes that the election officials are well known of the speculations of blockchain and can help the voters in the election process.

Yousif Abuidris et al., [16] proposed Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding which is a state-of-art electronic voting that uses Hybrid consensus model along with the sharding mechanism to secure the system and also uses Proofof-Stake and Proof-of-Credibility model to make nodes more powerful and create blocks efficiently. Smart Contract provides a trustworthy public bulletin board and secure environment to get accurate balance outcome. Coercion resistance and receipt freeness has to be included which is tamper-resistant source of randomness to establish users' ballot which can be disadvantageous.



PAPER NAME	AUTHOR	ALGORITHM MODEL USED	ADVANTAGES	DISADVANTAGES
A Conceptual Secure Blockchain-Based Electronic Voting System [17]	Ahmed Ben Ayed	SHA-256 algorithm	Provides ability to vote using any device and blockchain and is verified in such a way that it is immutable.	Liable to DDOS attack and make elections not accessable to voter. User can cast vote only once.
A Comparitive Analysis on E-Voting System Using Blockchain [18]	Kanika Garg et al.,	Cryptography model	Different approaches to tackle the anonymity, security, availablity, fairness verfiablility is discussed.	Does not cover authentication like biometric or unique ID.
Covid-19 Implementation evoting Blockchain Concept [19]	Mustofa Kamil et al.,	Cryptography model	Reduce the human gathering in elections during pandemic. Cryptographic protocol makes the results of votes transparent and safe.	Voting is not done effortlessly other than in public network as each transaction of vote takes 15 to 20 seconds.
Implementation of Auditable Blockchain Voting System with Hyperledger Fabric [20]	Michal Pawlak et al.,	Consensus algorithm	Hyperledger fabric focuses on providing high customizability, security and modularity.	Verifying the portability of ABVS model is not implemented.
A Systematic Review of Challenges and Oppurtunities of Blockchain for EVoting [21]	Ruhi Tas et al.,	Consensus algorithm, Proof-Of-Work and Proof-OfStake model, Governance model	Contributions made for the issues like integrity, privacy and consensus.	Usage of untrusted system, scalability attack, low transparency is not discussed.
Blockchain-Based EVoting System [22]	Fridrik Hjalmarsson et al.,	Byzantine algorithm, Proof-OfAuthority model	Smart contract is utilized to enable reliability and costeffective election as well guarantees voters privacy	Additional procedures has to be taken care of while conducting voting at large number transactions per second.





III. CONCLUSION

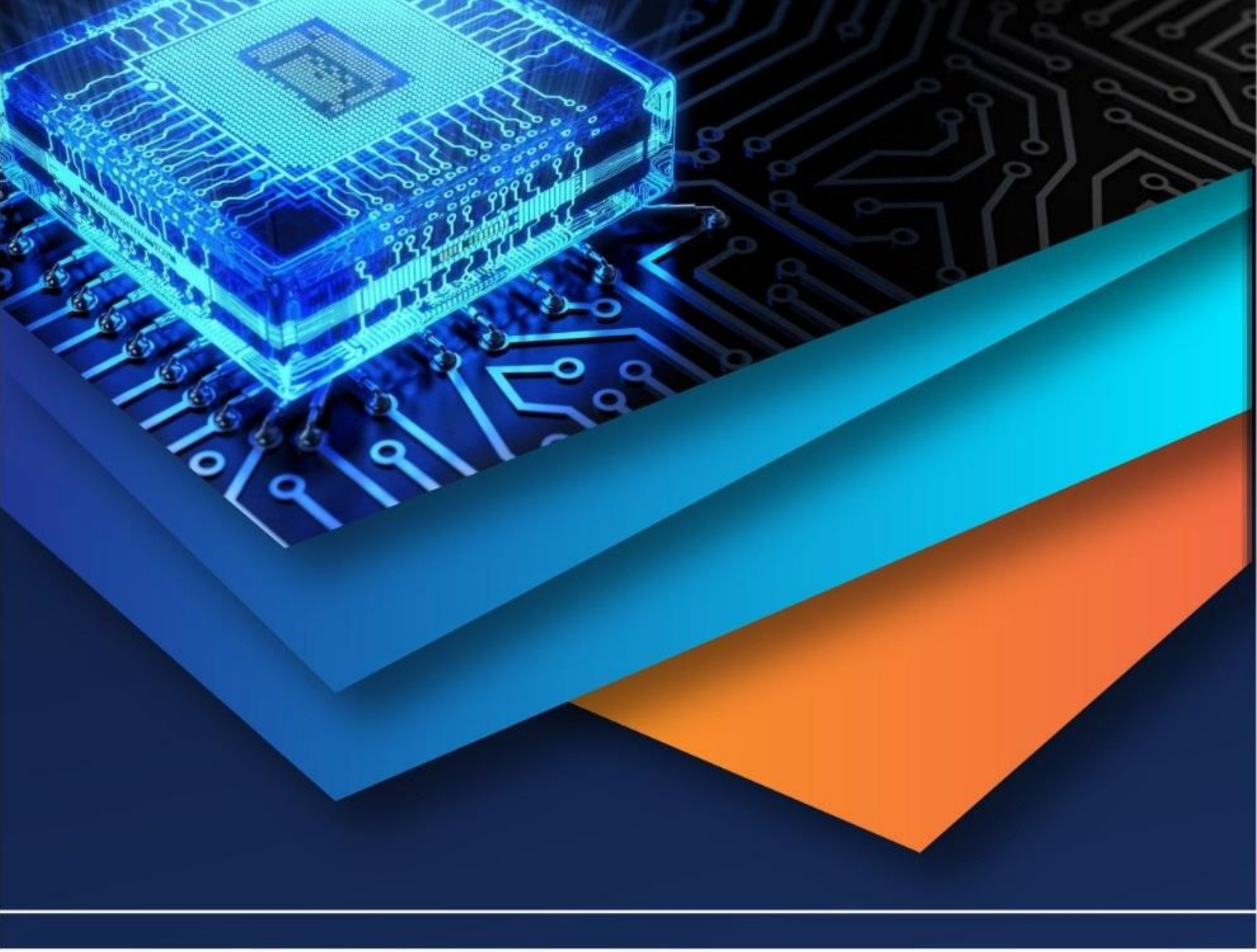
This paper demonstrates the secured blockchain based digital voting system. The framework shows that blockchain overcomes the disadvantages of the present voting model. Ethereum blockchain has been used as a part of the network along with Ganache which acts as the database to store the voters' accounts, information about the candidates and the votes that has been casted. In this way, blockchain allows us to create a transparent and secured voting model for digital elections.

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

REFERENCES

[1] Somnath Panja, Bimal Roy, "A secure end-to-end verifiable e-voting system using blockchainn and cloud server", Journal of Information Security and Applications, Vol. 59, June 2021.
[2] Jen Ho Hsiao, Raylin Tso, Chien Ming Chen, Mu En Wu, "Decentralized E-Voting Systems Based on the Blockchain Technology", Advances in Computer Science and Ubiquitous Computing, Vol. 474, pp. 305309, Dec 2017.
[3] Kibin Lee, Joshua I James, Tekachew G Ejeta, Hyoung J Kim, "Electronic Voting Service Using Block-Chain", The Journal Of Digital Forensics Security and Law, Vol. 11, Issue 2, Article 8, 2016.
[4] Ashish Singh, Kakali Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 863-867, Sep 2017.
[5] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract", 2020 Third International Conference on Smart Systems and Inventive Technology, pp. 228-233, 2020.
[6] Harsha V Patil, Kanchan G Rathi, Malathi Tribhuwan, "A Study on Decentralized E-Voting System Using Blockchain Technology", International Research Journal of Engineering and Technology (IRJET), Vol. 5, Issue 11, pp.48-53, Nov 2018.
[7] Abhishek Kaudare, Milan Hazra, Anurag Shelar, Manoj Sabnis, "Implementing Electronic Voting System With Blockchain Technology", 2020 International Conference for Emerging Technology, pp. 1-9, 2020.
[8] Md Razu Ahmed, F M Javed Mehedi Shamrat, Md Asraf Ali, Md Rajib Mia, Mst Arifa Khatun,"The Future Of Electronic Voting System Using Blockchain", International Journal Of Scientific & Technology Research, Vol. 9, Issue 2, Feb 2020.
[9] Kriti Patidar, Dr Swapnil Jain, "Decentralized EVoting Portal Using Blockchain", 2019 10th International Conference on Computing, Communication and Networking Technologies, pp. 14, 2019.
[10] Kashif Mehboob Khan, Junaid Arshad and Muhammad Mubashir Khan, "Secure Digital Voting System Based on Blockchain Technology", International Journal of Electronic Government Research, Vol. 14, Issue 1, pp. 53-62, Jan 2018.
[11] Haibo Yi, "Securing e-voting based on blockchain in P2P network", EURASIP Journal on Wireless Communications and Networking, Article 137, 2019.
[12] Ketulkumar Govindbhai Chaudhari, "E-Voting System Using Proof of Voting (POV) Consensus Algorithm Using Block Chain Technology", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 7, Issue 11, pp. 4051-4055, 2018.
[13] Camilo Denis Gonzalez, Daniel Frias Mena, Alexi Masso Munoz, Omar Rojas, Guillermo Sosa Gomez, "Electronic Voting System Using an Enterprise Blockchain", Institute of Cryptography, University of Havana, Havana 10400, Cuba, Vol. 12, Issue 2, pp. 531, Jan 2022.
[14] Xuechao Yang, Xun Yi, Surya Nepal, Fengling Han, "Decentralized Voting: A Self-tallying Voting System Using a Smart Contract on the Ethereum Blockchain", International Conference on Web Information Systems Engineering, Vol. 11233, pp. 1835, Oct 2018.
[15] Basit Shahzad, Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access, Vol. 7, pp. 24477-24488, Feb 2019.
[16] Yousif Abuidris, Rajesh Kumar, Ting Yang, Joseph Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding", Electronics and Telecommunications Research Institute (ETRI) Journal, Vol. 0(0), pp. 1-14, Nov 2020.
[17] Ahmed Ben Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System", International Journal of Network Security & Its Application (IJNSA), Vol.9, No.3, May 2017.
[18] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr Aggarwal, Sai Krishna Kothuri, Sahil Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoTSIU), pp. 1-4, April 2019.
[19] Mustofa Kamil, Po Abas Sunarya, Untung Rahardja, Nuke Puji Lestari Santoso, Muhammad Iqbal, "Covid-19: Implementation e-voting Blockchain Concept", International Journal of Artificial Intelligence Research, Vol. 5, No. 1, pp. 25-34, June 2021.
[20] Michal Pawlak, Aneta Pniszewska Maranda, "Implementation of Auditable Blockchain Voting System with Hyperledger Fabric", International Conference on Computational Science, Vol. 12742, pp. 642-655, June 2021.
[21] Ruhi Tas, Omer Ozgur Tanriover, "A Systematic Review of Challenges and Oppurtunities of Blockchain for E-Voting", Symmetry, Vol. 12, Issue 8, pp. 1328, July 2020.
[22] F P Hjalmarsson, G K Hreiosarsson, M Hamdaqa, G Hjalmtysson, "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986, July 2018.

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)