IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Privacy Preserving Voting Scheme Based on Blockchain Technology

Francis Shamili S[1], Pradeep M[2], Ravi Kumar R[3], Suren S[4], Vignesh K[5]
Assistant Professor, Department of Computer Science and Engineering[1]
Students Department of Computer Science and Engineering[2,3,4,5]
Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, India

Abstract: *Democracy has made voting incredibly important in any nation due to a general scepticism of the traditional voting process. Individuals have witnessed violations of their fundamental rights. Lack of transparency has led to challenges to other digital voting systems. The majority of voting methods are not sufficiently transparent, which makes it highly challenging for the government to win over voters' trust. The previous and present digital voting systems have failed because they are vulnerable to abuse. The main goal is to fix issues with the traditional and electronic voting systems, including any form of error or unfairness that may occur when voting. To ensure a fair election and lessen unfairness, blockchain technology can be included into the voting process. The computerised voting methods are not flawless enough to be used on a broad scale, and the physical voting systems have numerous problems as well. This evaluates the requirement for a remedy to safeguard citizens' democratic rights. In order to establish a trustworthy working connection between voters and election officials, this article introduces a platform based on cutting-edge blockchain technology. Without using any actual polling places, the proposed technology offers a framework that may be used to conduct voting activity digitally through blockchain. Our suggested design uses adaptable consensus algorithms to support a scalable blockchain. Blockchains with pre-established validation procedures were developed for a specific voting storage.Voter verification will be provided by IRIS Recognition. All systems in a value chain save blocks of time-stamped voting. Blockchain is a log of transactions where members of a community may track asset transfers. Using the SHA-256 technique, two blocks are connected to one another. It has also been elaborated on how to encrypt transactions using cryptographic hashes and guard against 51% attacks on the blockchain. Also, the method for conducting blockchain transactions during the voting process has been developed using Blockchain Lastly, the performance assessment of the suggested method demonstrates that it may be used to a sizable population.*

Keywords: E-polling, voting system, blockchain application, blockchain voting, E-voting, electoral system, blockchain, cryptographic hash, secure voting

I. INTRODUCTION

Through establishing the areas, hiring staff, and reducing security concerns at polling places, blockchain can significantly cut the time and money spent on polling places [1]. Blockchain-based digital elections provide for cost savings while lowering the possibility of unfair votes [2]. If handled wisely, modern technologies like blockchain technology are very secure and helpful. It can improve transaction traceability, voting system reliability, and transparency [3]. A voting machine that is connected to a centralised database has been utilised in traditional digital voting methods. A person with physical access to this device has the ability to tamper with it. The voting system's entire network may experience a single point of failure as a result; whereas, an immutable blockchain wouldn't be impacted by a single network saboteur [4]. Data is decentralizedly kept on a blockchain, where the accuracy of the records is continuously verified. As a result, if a node were to be the objective of a malicious attack, just that node would be impacted, and the peer-to-peer network would keep providing all services. As a result, blockchain technology may be used as a secure and trustworthy private ledger in voting systems. More security and trust may now be achieved with

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

blockchain than with previous systems [5]. Less staff can be hired, security personnel can be reduced, and polling places for a conventional voting system can be set up for the miners [6].

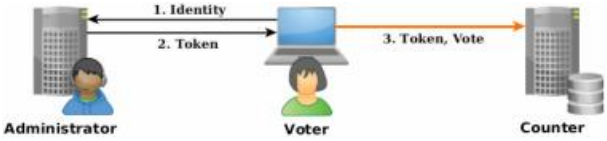

Figure 1.Traditional voting system.

It doesn't need a real voting machine or module, which is always vulnerable to hacking through tampering tools [1]. The most interesting facet of this method is its transparency, which gives voters confidence that their votes are being cast in the most appropriate ways. Compared to traditional databases, blockchain technology is more transparent and secure. Critical systems like banking, healthcare, food safety, and cryptocurrency exchange are being examined for deployment [6]. More security and trust may now be established by blockchain than with earlier systems [5]. Saving the resources is possible. In comparison to previous digital voting systems, the voting system will be more accurate, secure, and consistent if blockchain technology is used. Voter privacy and trust may be secured while a transparent voting method is used using blockchain technology, requiring less staff, security officers, and other resources.

II. RELATED WORK

Introduced a blockchain-based digital voting system that could be applied in an environment using advanced technology. The system that made the notion that all of the connected object was reliable. The system's security weaknesses, however, are of significant concern because they could allow for the rigging of votes by intruders. In contrast, our suggested voting solution reduces the possibility of intrusion by using encryption and secure networks. The system presented by M. Pawlak et al. [15] does not need any operating entities. It also required extensive computing and was unable to secure a voter's identity. The system was able to gather user votes, but because of complicated computation, latency started to become a problem as the user rate increased. Identification of the Voters became exposed. The system was unable to process a sizable volume of data; as a result, large-scale implementation was not successful. While in our suggested voting system, latency is controlled through the flexible application of consensus procedures.

Blockchain's use of cryptographic hashes eliminates the possibility of voter identity being exposed. The robustness and fairness of the vote tally were improved by a proposed system by D. Chaum et al. [16]. Voters now have the option of end-to-end verification to ensure that their votes are included in the final vote total. Each voter had the ability to check if their vote had been counted and accurately recorded. A special code was provided to each voter, which they could use to enter into the system and confirm their vote.Voters can use their registered phone numbers and email addresses to confirm their ballots. Voter confidence is increased .He asserted that if implemented properly, internet voting via blockchain may provide positive outcomes. They talked about certain technical issues with electronic voting methods. The system's robustness was uncontrollable. When end-to-end verification is used, the error of double-registering users is minimised. Low latency voting systems that did not protect voters' privacy were used. The suggested blockchain voting system uses smart contracts and a flexible consensus method to reduce system latency.A thorough comparison of our suggested VMS and alternative voting systems based on blockchain technology is provided.Our suggested system offers a flexible consensus method at run time that helps to govern the performance of the voting activity, unlike the state-of-the-art blockchain voting system, which was built on a single fixed consensus algorithm. To stop harmful activity during the

III. PROPOSED FRAMEWORK OF VOTING SYSTEM:

Unlike other programming fabrics where an director can add, cancel, or change the data, blockchain is malleable. Anyone with access might tamper with the system and alter or remove the votes if such a system was executed for voting. The blockchain technology changes this. A knotcan not be changed or deleted once it has been added to the chain, under any circumstances. The chain becomes inflexible if a knot is attacked by an bushwhacker and the other bumps descry it and repair the damaged knot. The voting system is independent of any specific calculating knot thanks to the simplified nature of the blockchain. Indeed if one or further bumps are attacked or go down, the voting process

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

still goes on as usual. Under every grueling circumstance, it ensures responsibility. Choosers, Identification Authorities(IA), and the Administration Authority(AA) of the electoral commission are the major actors in the proposed system.

A. Voting System Architecture

The planned system's high- position structure has been handed. It demonstrates how the crucial actors — Choosers, VMS, AA, and IA — unite to carry out specific voting duties. Via dAPP, which can be either a mobile operation or a web gate, all choosers are incontinently connected to VMS. Choosers registered in the system are vindicated by the identity authority. Each namer who has been vindicated as being eligible to bounce may share in advancing through the operation. The stoner interface of the operation is the first element of the whole system process, and it also needs frontal- end security. Because the stoner enters his credentials on that interface.

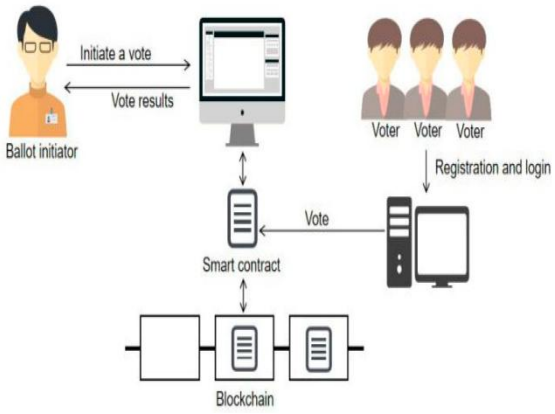

Figure 2. Voting system architecture

Every stoner has full and indifferent access to the system throughout voting exertion. also, it offers traceability after a vote has been cast. By using his credentials, the namer registers in the system. In order to register a namer in the system, VMS uses the information on their ID and confirms it against IA's online database. A distinct OTP is transferred to the stoner to enable system access. Every time a namer tries to log into the VMS, an OTP is generated. The namer's complete information is saved in the VMS. Each namer receives One Voting Coin(VC) after successfully. Registering with the system.to enjoin people from casting a ballot each namer receives just one VC, not doubly.

B. Work Flow of Proposed Model

The seeker is added to the Voting Control System after complete the verification. On the blockchain, a single chain system is put into use. To maintain the integrity of the namer's vote, the system is also integrated with the nation's public database. A sale is created against the namer's National ID for each vote. The small beach kept in the blockchainis also used to booby-trap the sale. Vote Currency from the namer's portmanteau is also used throughout the voting process. Once one vote coin has been used, the namercan not cast anothervote. However, the request will be rejected and the namer will be logged out of the system, If a transfer hash matching the namer's done National ID is discovered. The request to add the knot is given to the miner if a namer has not yet cast their ballot. The namer makes his choice of seeker and also casts his ballot. The sale is carried out by the miner and is tracked with the aid of a sale hash. The knot is also connected to the voting chain. To share in voting, choosers has to have a mobile device or web cybersurfer. In order to make the namer's interface accessible to all druggies, multiple languages would be offered. At the time of voting, the suggested system has the capacity to accommodate numerous choosers.

C. Layered Structure of the Proposed VWS:

The suggested framework will be provided in layers. The process of All of the voter and administrative dAAPs are contained in the interface layer. These are the widely available applications that allow any stakeholder to connect to VMS. This layer's objective is to offer a means of engaging with the system. Application Layer uses outside resources to provide a user verification method. It is the voting system's front-end user interface. It stores the voting system's data in internet databases. This layer also manages all blockchain transactions. A user's eligibility to participate in this voting

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

activity is confirmed using his or her national identification. The most crucial component of the entire structure is the Trust layer.

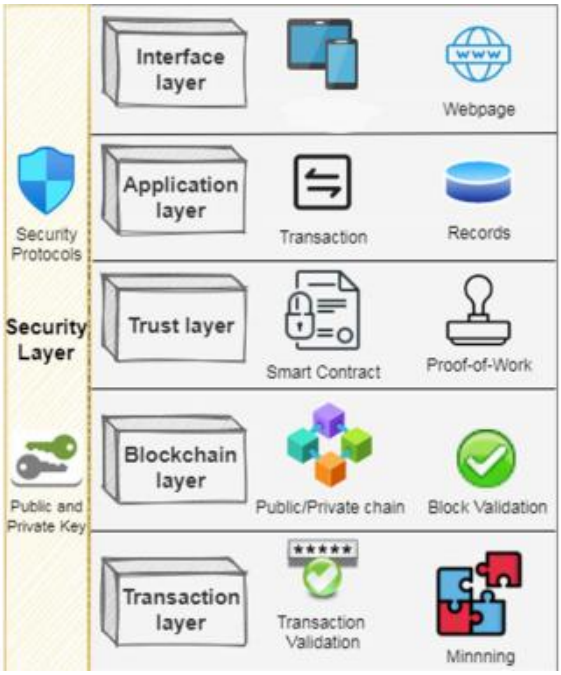

Figure 3. Layered structure of the framework

It guarantees that the right consensus is reached and that data is transferred securely via smart contracts. Each new block that is added to the chain is itverified. The blockchain layer stores the fundamental data connected to the blockchain and keeps track of any problematic nodes to guarantee the chain's immutability. This layer stores all of the transaction data, including the public and private keys.All activities between VMS and voters that employ smart contracts are included in the transaction layer. The transaction layer is where all transactions are mined. The security layer, which guards the blockchain against attacks, is the most important layer. Algorithms and fundamental principles that make it difficult for outside entities to harm the chain are used to defend against any attack attempt. The entire chain is using the security procedures. Data across the system is encrypted and protected thanks to the private and public keys.

D. Flexible Consensus Algorithm:

The suggested framework is compatible with scaling blockchain. The system offers plug-and-play consensus algorithm support. To maintain the blockchain's efficiency throughout the voting process, the Proof of Work agreement method has been suggested by default; however, the framework also supports other consensus protocols that can be selected at the time the blockchain is deployed. A transaction has used a specific amount of processing power, according to Proof of Work.

The framework is adaptable enough to take into account a run-time change in consensus algorithms. It contributes to the block chain's security and preserves uninterrupted voting. The blockchain performs best at runtime when an appropriate consensus algorithm is selected at deployment time. There are numerous consensus algorithms that can be used. Ripple, Proof of Vote, Proof of Trust, and Proof of Stake are all used in voting. By verifying random nodes, Proof of Stake in this case determines how much processing power the system needs. A node immediately loses its stake in the voting chain if it is validating a bogus transaction. These nodes' transactions are rejected.

IV. DESIGN &IMPLEMENTATION

The voting process is managed by our system, which is supported by the blockchain. Every voter's transaction hash is kept on the chain, and all election results are likewise stored there. From there, users can access the election results dashboard to view the outcomes of the election. The voting system first confirms that the voter is the nationality holder

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

of the country and determines whether or not the voter has already cast a vote. If the voter still has a vote coin, the voting system permits him to cast a vote. The voter identifier, vote, and timestamp were stored in the chain that stores vote details after being verified. The entire procedure is detailed.

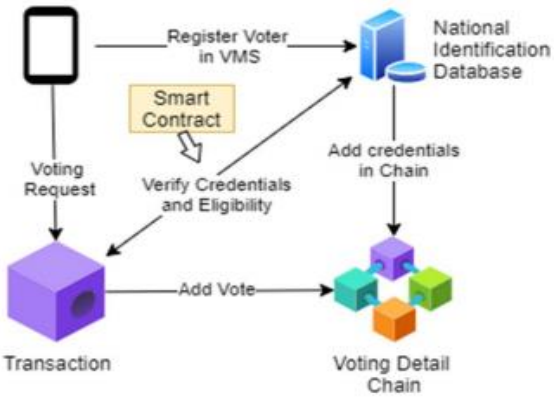

Figure 4. Smart contract.

4.1 dAPP Setup

The many parts of the voting management system are covered in this section. Voters can engage securely with the system using a user interface that also provides front-end security. The front end of the VMS has been given a lengthy time interface. A decentralised application built on blockchain technology is known as a web application. It utilises a blockchain P2P network to operate. Because the user enters their credentials on that interface, user identification is crucial and Every must be uncompromised.

voter has unequal access to the system, which also enables traceability of votes cast. The voter uses their credentials to log into the system. In order to register a user in the system, the system takes the user's ID information and verifies it against the database. The dAPP technology is used to guarantee VMS stability since decentralisation makes processing effective at all nodes. The other nodes of the system are not damaged if one becomes insecure during the election process. The insecure node is restored by the other networks.

4.2 Uniqueness of Voters

Users' computerised National IDs can be used to determine their individuality. Voters' information is first entered, and then it is validated with the help of recognizing authority. This ensures that yet another person is not using a person's identity. By requesting permits, the authorities can determine if a person is entitled to participate in the vote and whether his or her National ID has already been associated with any transactions. If a voter is qualified, the system registers them and gives each voter account one Voting Coin. By using this approach to confirm the user, the system can also determine whether the user satisfies the conditions set forth by the legislation and casts a ballot. A process identifier is provided to the voter's Personal Username when they cast their ballot. Moreover, the wallet status of voters is changed to zero voting coin, removing the possibility of a person casting two votes at once. The blockchain updates and saves a voter's vote as they cast a ballot, therefore unless a fresh VC is granted, the user cannot cast another ballot.

4.3 Electio as a Smart Contract

While carrying out a transaction in the blockchain, smart contracts are offering a safe link between the user and the network. These are the regulations that apply to the entire blockchain and cannot, under any circumstances, be disregarded. To successfully save the vote in the system, all nodes must adhere to the smart contracts. The Can-Cast-Vote function, which verifies that the provided voter is eligible to cast a vote, is used in the first smart contract to verify users between the IA and the VMS. It enters the voter information record after verification for later usage. A voting smart contract that indicates which candidates will be displayed to the voter is tied to the voter. Voting is permitted if the consensus reached by the node and the chain is in agreement. The system's smart contact to cast a vote. It determines whether the voter is eligible to cast a ballot by looking at the Vote Coin in his or her wallet. a feature Voters'

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

National IDs and wallet addresses are inputted while casting a ballot, and a check is made to see if the user voting coin is authorized. The voter may only cast a vote if they have a voting coin; otherwise, the vote request is refused by the smart contract. Using a cryptographic hash, all the data contained in the transaction is securely encrypted.
The voter is directed to a fresh screen to enable him receive the proper voting guidelines if the agreement does not match. Perhaps the ID is incorrect or the person isn't allowed to vote for some reason. Each voter is provided with a wallet that holds just one Voting Coin. The wallet is lowered by one after a transaction made and is left empty. That guarantees that voter won't be allowed to cast another ballot.

4.4 Transactions in VMS (UTXO)

The idea of Unspend Transaction Outputs (UTXO) in the suggested system is explained in this section. Each voter receives one VC in their wallet at the moment of registration, as was covered in Section IV Part C. It can only be used once to cast a ballot for candidates. UTXO is a method used in VMS to carry out voting transactions. Each transaction costs 1 VC to complete. The miner receives this VC as payment. Since the method maintains the equality of all voters' rights, there are no transaction fees in the voting process. Voter1 spends 1 VC to support Candidate2 in the election. This transaction is noted and sent to the transaction memPool. Miners begin mining after picking up several transactions from there. Here, every transaction updates the value of UTXO to zero, making it impossible for a voter to cast another ballot.

4.5 Cryptographic Hash

Cryptographic hashes, which also protect stoner identity confinement, keep the data hidden from any system intrusions. Only the permitted owner of the process can unlock it and view the content using his secret key. In order to keep the transaction secure when it is transferred on the network to be added to a knot, cryptographic hash uses encryption. The stoner's vote can be tracked by providing the namer with his sale address; the namer is notified via SMS and notified as impolitely as the vote is made. Choosers can conceal their vote on the blockchain by employing the hash law of the process that is provided on the phone number recorded.
The information gathered during the voting procedure is included in the vote data. The data is still secret, protected, and safe. The only person who has access to the shadowing data is the namer, who may also check his or her voting history. After the process has been saved in a block, it is locked using the namer's public key. When recording the vote, the knot is identified using the namer's public key. The namer uses his private key to view the transactions his portmanteau has made. Voters can only observe their ballots; once they have been cast, they are unable to amend or annul them. All data exchanged during a sale of marijuana is encrypted using cryptography.

4.6 Chain Deployment

The chain deployment is described in detail in this section. The voting record is mined further into blockchain after the voter casts their ballot in the system. The voter is alerted of each successful blockchain transfer via the registered phone number. Using the transaction's hash code, the voter can confirm that his vote was cast. Only successful transactions are processed by the chain to determine the voting outcome since only those votes are considered. This way of changing the status of vote transactions on the chain solves the problem of the partial process transactions. To deal with the volume of transactions on blockchain, a 10-minute delay has been chosen.
The results of the vote can be seen by election officials on the VMS dashboard after voting.Election data, voters, and qualified candidates. The low literacy rate in any nation can be a weakness of the system, but it can be fixed by distributing recommendations through the media and preserving the user interface as straightforward as possible. The technology also specifies a multilingual user interface that voters who speak the language can utilise with ease. The sole threat to the voting system's security is a miner's or a group of miners' 51% control on the hash rate.

4.7 Preventing Attack 51%

Controlling the blockchain's 51% hash rate is the goal of the 51% attack. A extremely high amount of processing power is needed to reach this hash rate. Two solutions in VMS prevent 51% of attacks. First off, the system has already registered each miner's hash rate. In a blockchain system, hash rates are watched to see whether any miners do not have

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

a 51% hash rate. A user who violates this rule is prohibited from mining while the vote is being cast. Second, the voters are pre-selected from among the miners. Under the direction of authorities, miners are employed to mine while elections are taking place. The vote process is not permitted to involve any outside mining groups. The network prevents any rogue miners from mining a block in the chain when the system is always being watched over during voting activity. The system detects any voting action and prevents pre-selected miners from rejoining the chain if they leave the mem-pool. Whenever any fraudulent activity takes place or a miner attempts to add a bogus block to the chain that is not validated, a 51% assault is proclaimed and mining activity is suspended in order to maintain it completely secure and tamper-proof. The network is dominated and won by nodes with longer linkages. Nodes could join the network even without Voting Authority's authorization since the blockchain is allowed. A group of compromised nodes could join at runtime without having their credentials and access verified. Thus, the proposed method does not allow for a 51% attack.

VI. CONCLUSION

Building confidence between the government and the electorate was the goal of the blockchain-based voting system proposal, which was intended to give voters the impression that their voting integrity was protected. Voting on the blockchain also makes the process transparent and reliable. The cost of voting in any nation is very high when utilising the old voting method, but the proposed alternative would use blockchain voting technology to make voting cheaper, faster, and more reliable. People's relationships with their democratic state are improved as a result since they have a transparent system they can rely on. In order to raise the level of the electoral system and increase its dependability, traceability, and confidence, the framework elaborates on the features, services, and role of official authorities using blockchain in the voting system. Each vote is verified, making the results immutable. The concept of public and private keys enables the administration to precisely control the process while the usage of hash ensures the anonymity of voters.

The voting system's traceability helps guard against hackers accessing or changing the voting data. It ensures that each voter casts a single ballot. By employing the more efficient method of developing a flexible consensus algorithm to cut down on the enormous processing resources in the blockchain, the usability of this system performs well. Voters may likely rely on and trust the system because of its open behaviour. Moreover, the Chain Security Algorithm, which automatically validates the chain's legitimacy each time a new block is added to it, is included.

Smart Contracts are crucial in ensuring that the blockchain voting system doesn't contain any fraudulent or incomplete transactions. The suggested system provides voters and government officials with a safe, transparent, and trustworthy platform. Based on an assessment of how well the suggested framework uses blockchain technology in VMS, the results look promising. The experiment demonstrates that the system maintains efficiency even when handling a significant volume of blockchain transactions.

REFERENCES

[1]. Kumar, Mahender, Satish Chand, and ChittaranjanPadmanabhaKatti. "A secure end-to-end verifiable internet-voting system using identity-based blind signature." IEEE Systems Journal 14, no. 2 (2020): 2032-2041.

[2]. Mansingh, PM Benson, T. Joby Titus, and VS Sanjana Devi. "A secured biometric voting system using RFID 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1116-1119.IEEE, 2020.

[3]. Wang, Zikai, Xinyi Luo, Meiqi Li, Wentuo Sun, and KaipingXue. "WeVoting: Blockchain-based Weighted E-Voting with Voter Anonymity and Usability." In GLOBECOM 2022-2022 IEEE Global Communications Conference, pp. 2585-2590.IEEE, 2022.

[4]. Li, Meiqi, Xinyi Luo, Wentuo Sun, Jian Li, and KaipingXue. "AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain." In ICC 2022-IEEE International Conference on Communications, pp. 4751-4756.IEEE, 2022.

[5]. Shahzad, Basit, and Jon Crowcroft. "Trustworthy electronic voting using adjusted blockchain technology." IEEE Access 7 (2019): 24477-24488.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

[6]. Adekunle, Salako E. "A Review of Electronic Voting Systems: Strategy for a Novel." International Journal of Information Engineering & Electronic Business 12, no. 1 (2020).

[7]. Faruk, MdJobair Hossain, Mazharul Islam, FazlulAlam, Hossain Shahriar, and Akond Rahman. "Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework." In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp. 253-258. IEEE, 2022.

[8]. Okokpujie, Kennedy, John Abubakar, John Samuel, Etinosa Noma-Osaghae, Charles Ndujiuba, and Imhade Princess Okokpujie. "A secured automated bimodal biometric electronic voting system." IAES International Journal of Artificial Intelligence 10, no. 1 (2021): 1.

[9]. Ahmad, Masood, Ateeq Ur Rehman, NighatAyub, M. D. Alshehri, Muazzam A. Khan, Abdul Hameed, and HalilYetgin. "Security, usability, and biometric authentication scheme for electronic voting using multiple keys." International Journal of Distributed Sensor Networks 16, no. 7 (2020): 1550147720944025.

[10]. Prof. Pathak Neeru1, Gite Swapnil2, Pawar Amruta3, Sancheti Sumit4 "BIOMETRIC BASED ELECTRONIC VOTING SYSTEM" International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 04 | Apr 2020

[11]. Farooq, Muhammad Shoaib, UsmanIftikhar, and Adel Khelifi. "A framework to make voting system transparent using blockchain technology." IEEE Access 10 (2022): 59959-59969.

[12]. Dimitriou, Tassos. "Efficient, coercion-free and universally verifiable blockchain-based voting." Computer Networks 174 (2020): 107234.