Semiconductor Optoelectronics
ISSN: 1001-5868

DECENTRALIZED E-VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGYUSING SMART CONTRACTS AND KECCAK-256 ALGORITHM

Mr M. Imrankhan[1] , S. Sakthivel[2], R. Logeshwaran[2], Sangadi jayaram[2], K. Nandhakumar[2]

[1]Assistant Professor, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India.

[2]UG student, Manakula Vinayagar Institute of Technology, Puducherry, India.

ABSTRACT: The potential of blockchain technology to solve the most common problems associated with traditional voting systems has been presented. Through the use of smart contracts, the developers of these systems have been able to greatly reduce the number of issues related to fraud and tampering. A blockchain- based system for voting can offer various advantages. It can provide a secure and anonymous method of voting,and it can be recorded on the blockchain. Moreover, smart contracts can verify that only eligible voters participate in the process. A blockchain-based system for voting could enhance transparency, efficiency, and integrity while fostering trust in the democratic process. In this system, we use smart contracts to connect our soft wallet to a smart contract for transactions. The blockchain technology's promise to promote transparency and efficiency the voting process in immense. It could also foster trust and confidence in the democratic process itself. In this system, we use smart contracts for the exchange of tokens.

INDEX TERMS -Blockchain, Smart Contracts, Keccak256, Ganache.

1.INTRODUCTION

The rise of blockchain technology has created a revolutionary new way to manage information and transactions. It can also help create trust in digital environments. One of its most prominent applications is the development of e- voting systems. These systems promise to enhance the security, transparency, and accessibility of voting processes, and to mitigate some of the challenges and risks associated with traditional voting methods. A blockchain is a type ofdigital platform that enables people to vote using a secure and verifiable method. The system is based on a decentralized network of nodes, or computers, therefore they can communicate with each other to validate transactionsand maintain a shared database of all votes cast. This database, or Immutable, which means that once a vote has beenrecorded, it can't be deleted or altered without the consensus of the network.

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transactions Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transaction size.

Table 1. Structure of the Blockchain.

One of its main advantages is that it allows people to keep track of their transactions in a decentralized manner. Because the system is decentralized and uses cryptographic protocols to validate transactions, it is virtually impossiblefor any single entity to manipulate the results or hack into the system. This is particularly important in contexts wheretrust in traditional voting methods is low, such as in regions with high levels of corruption, or in countries where election fraud has been reported. Another advantage of blockchain voting systems is their transparency. Since all of the transactions are stored on a blockchain, anyone can inspect and verify the results of the vote to ensure that they are correct and accurate. This eliminates the risk of errors and provides for greater accountabilityMoreover, blockchain systems make it easier for voters to use. With traditional voting methods, voters often have to travel to a physical polling station, wait in long lines, and fill out paper ballots. This can be particularly challenging for people with disabilities or those living in remote areas. With blockchain voting, however, voters can cast their votes securely and along from their own devices, eliminating the need for physical polling stations method and reducing the barriers to voters.

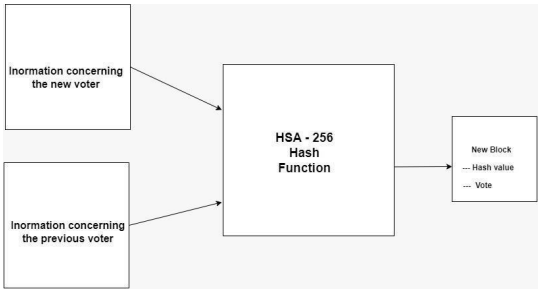

Fig 1 Creating of new Block containing a Hash Value and a vote.

Keccak 256 Algorithm:

To generate distinct IDs for transactions, smart contracts, and other data recorded on the blockchain, the Ethereum blockchain uses the Keccak256 algorithm, a hash function. This technique, which generates a fixed-size output of 256bits, is a one-way function and a part of the SHA-3 family of hash functions. When using the Keccak256 algorithm, an input message of any length results in a fixed-size output of 256 bits. The input message is initially extended withextra bits to make it longer than 1088 bits, the internal block size of the algorithm. The padded message is then dividedinto 1088-bit blocks, and the algorithm executes on each block in turn.The method consists of a sequence of phases that use bitwise operations like XOR, NOT, and AND as well as permutation functions that mix the input's bits. For each block of

the input message, these processes are repeated until the complete message's hash is produced as the final output.

Fig.2 Basic function of the SHA-256 Hash.

The Keccak256 algorithm is utilized in the Ethereum blockchain in a variety of ways, including to generate the uniquetransaction identification that is then recorded in the blockchain. The hash of the transaction data, which includes thesender, receiver, and amount transferred, is used to create this identification, which is referred to as the transaction hash. In conclusion, by creating distinctive IDs for transactions and smart contracts, the Keccak256 algorithm significantly contributes to the security and integrity of the Ethereum blockchain. It is a safe and dependable techniqueof data authentication and verification because of its one-way function, which makes it impossible to reconstruct the original input message from the hash.

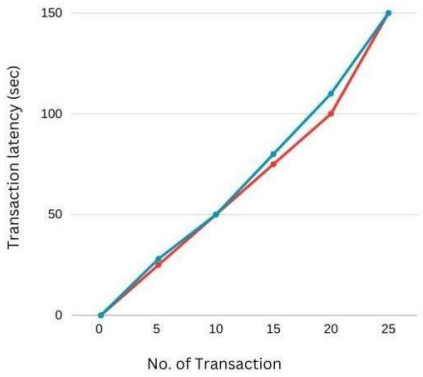

Fig .3 No. of transactions.

Blue indicates the keccak 256 Transactions Latency sec.Red indicates the SHA 256 Transactions Latency sec.

SHA-256 and keccak-256 are two of the most widely used hash algorithms for a variety of purposes, including crypto currencies. Despite the fact that they are both quite secure, the former is seen to be more effective at handling transactions. Keccak-256 is a more effective transaction processor when compared to SHA-256. For high-volume applications, it can process more transactions per second. Moreover, SHA-512's internal processes are distinct from those of SHA-512, making it more difficult to attack. Generally, Keccak-256 is regarded as a more safe and effectivesolution for a variety of applications, notably in the world of cryptocurrencies, despite the fact that both algorithms are frequently employed.

3. LITERARY SURVEY:

Decentralized E-Voting Portal Using Blockchain. Kriti Patidar, Dr. Swapnil Jain. . This paper makes a proposal for anelectronic voting system based on blockchain that gets rid of some of the drawbacks of current voting methods. The study also discusses the current state of different blockchain frameworks for electronic voting. Small-scale elections within corporate buildings, boardrooms, etc. are appropriate for the implementation that is being presented.
Decentralized E-Voting System Using Blockchain. Dr S. Sekar, C. Vigneshwar, J. Thiyagarajan, V.B. Soorya Narayanan, M. Vijay.The goal of this paper is to develop biometric voter confirmation, dynamic ballot loading, and post-voting acknowledgement utilizing blockchain technology in order to overcome the limitations of the current e- voting system.
Blockchain Based E-Voting Recording System Design. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang.The paper aims to introduce blockchain architecture and then compare the various consensus techniques used in different blockchains.
Secure Digital Voting System based on Blockchain Technology. Rifa Hanifa Tunisia, Budi Rahardjo.This research discusses the recording of voting results using blockchain algorithms from every place of election. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Syada Tasmia Alvll, Mohammed Nasir Uddin, LintaIslam, Sajib Ahamed.The possibility of decentralised voting is examined, as well as anumber of related concerns, including those relating to accuracy, privacy, and integrity.
Blockchain for Electronic Voting System Review and Open Research Challenges. Uzma Jafar, Mohd Juzaiddin Ab Azizand Zarina ShukurThe article examines the various facets of blockchain-based, decentralised electronic voting. It intends to examine the current state of this type of system's research and its potential future development. Decentralized Voting Platform Based on Ethereum Blockchain. David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb.With the use of Blockchain technology, we created a decentralised and secure voting system that addressesnumerous trust challenges. It has features that guarantee accuracy and openness and keep voting anonymous by onlyallowing one vote per cell phone number.

4. EXISTING SYSTEM

Estonia I-Voting System: Voters in Estonia may cast ballots using an electronic ID card that was connected to the Internet and had a Java chip and an integrated circuit. The card has the ability to produce SHA1/SHA2 signatures. Thecard is simple to use for signatures, encryption, and authentication. A list of candidates will be provided if the voter is qualified to cast a vote after downloading the voting programme and authenticating with an electronic ID. The vote will be sent to an Estonia government-controlled server after it has been cast, and only the results will be regarded asvalid. Multiple voters can cast their ballots, and only the ballots with the greatest number of valid votes will be counted. Norwegian I-Voting System: In 2011, Norway experimented with electronic voting for local government elections. This technique was almost identical to the Estonian improvement in e-voting produced by e-voting provider Scytl; however, they dismissed it four years later with security concerns. The primary reproads were primarily due to a potential of leaked votes should there ever be a successful cyber attack taking place.
New South Wales iVote System: In 2015, over 280,000 voters in New South Wales used the

iVote system to cast their ballots. Although the system was created by Scytl, it had a different layout. In order to use the system, citizens must go through four steps. Two of these are optional.

Rules for voting process:

- The voter must register with the authorities, get a voter identification card, and select a six-digit PIN.
- The voter enters his ID and PIN to log onto the system, casts his ballot, and then receives a 12-digit receipt number as proof.
- To make sure his vote was cast, the voter inputs his identification, PIN, and receipt number. This step is notrequired.

D.C Digital Vote-by-Mail Service: In 2010, the District of Columbia created a prototype of its own electronic votingsystem. In order to test its security, the city conducted a mock election. The project was abandoned when several serious problems were discovered, and it was never used in any formal elections.

Drawbacks and security issues: The Estonian and Norwegian electronic voting systems have been subject to significant criticism related to the concealment of essential aspects of their codes. There have been doubts raised concerning its openness due to how intricately set up it is for registers in the Estonian I-Voting system. A dependableelection necessitates an open-source electronic voting method. Because it's organized centrally, the I-Voting system is a target for DDOS strikes, which can thwart voters from executing their votes. Intelligence Agencies have the necessary capabilities to assess changes or other alterations that could have occurred in voting data. Even if augmented safety protocols are established, State level intrusions can still target the technology which was discussed previously.We shall suggest a strategy in this study concerning an e-Voting framework which uses open-source codes and is advanced amongst Blockchain technology to obtain votes while further decentralizing it.

Proposed System architecture: The system consists of three major components: one permanent and two removable that can easily be updated. This ensures the greatest possible user experience while minimizing vulnerabilities.

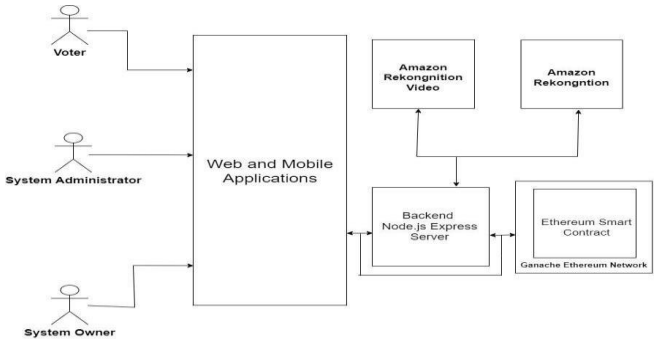

Fig4. System architecture.

First, the smart contract running on the Ethereum network guarantees real voting, validity and permanence of transactions before display of results. This system component is crucial, because it supplies independent features thatare crucial to an e-voting system. Furthermore, this element cannot be replaced by another one. Human face and emotion identifiers can be used to authenticate users, whether it's for hardware- or software-based authentication.

Smart Contracts: The smart contract was developed in Solidity and is constructed as abstractly as feasible to guarantee that it will be able to allow integration independent in terms of authentication modifications employed.

Admin: The construction the admin field holds the name of the person in charge of operating the system. It will log the administrator's status, which can be disabled if they fail to complete their obligations correctly. It also contains permissions that are only granted for the "moderator" and "owner" roles.
Option: A framework that represents the many voting propositions is an alternative. It makes no difference if the creator is a real person or not. This structure can also include information about the person who developed it, such asthe name of the party to which the choice belongs and the number of votes gained by other users via this option. This option's value will progressively rise from zero to one.
Voter: An option is a framework that reflects the numerous voting proposals. It makes no difference whether or not the creator is a human. This structure may also include information about the person who developed it, such as the name of the party to which the choice belongs and the number of votes gained by other users through this option. This option's value will progressively rise from zero to one. The voter detail's structure is intended to keep the user's information private. It includes the voter's name as well as unique identification data like their Social Security number. The structure of the voter details will not be disclosed. It is solely required for authentication and registration purposes. We feel that these aspects should be addressed regardless of the sort of vote being held.
System states: The Ethereum network's smart contract is immutable, which means it cannot be modified. Furthermore,because its transactions are neither changing nor reversible, the system must transition through various states. To transition between states, we'll need global variables, collections, and data types that allow us to do so. The contract'sfirst version only permitted the owner to see it. Although the owner has the option of moving to another state, his primary activities are to add new voting options, deactivate an administrator, and make modifications to the voting system. These three alternative activities become accessible only once the voting round has begun. Administrators canalso allow their users to vote by using their rights. Users must follow a certain procedure in order to participate in thevoting process. They must first join up, give their details, and have their account validated by an administrator. Theycan then utilise the "voting" process to select their preferred alternative. The voting phase will conclude, and the contract will be sent to the next, closed state. In this state, voters will only have two options: consider the outcomes, or shut off the system. The owner can prohibit the other two characters from engaging with each other by shutting thesystem.

5. BACKEND SERVICE

Users will be able to access and request information about the app's many features using a backend service. It is developed on top of the open-source Node.js Express Framwork. A controller exposes a group of submodules and services to the public via the API. The API is designed in a modular fashion. It can be used normally. For example, inorder to establish secure

communication, a client will first contact the key exchange endpoint. The login endpoint will then be called, and two base64-encoded pictures or URLs will be sent to an Amazon Web Services bucket.

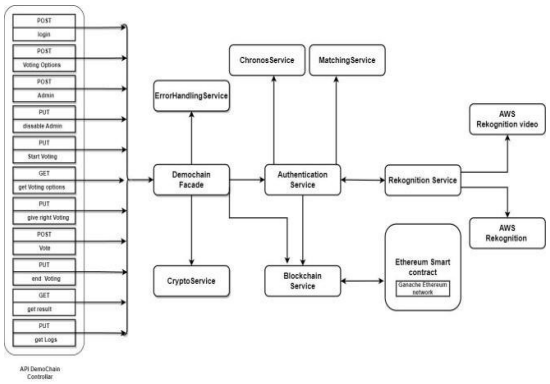

Fig5. API architecture.

When a service request is made, it is routed through a request processor, who intercepts the payload and calls an authentication service. This is part of the service's job as a liaison between different components. The first step is to use the Amazon Rekognition recognition service. The request will be forwarded to Amazon for examination and thenreturned to the authentication service. This procedure will next determine if the people in the photo match the peopleon the ID card. If this is not the case, the customer will be advised of the issue. The service will then investigate the data assessment chain to ensure that the other persons in the framework are likewise associated to the voter. It will examine the individual's facial expression to determine whether or not they are in danger. The different tests carried out are rigorous, and any problems will be reported. Optical character recognition is then used to establish the voter'sinformation and identity. The solution the current data will then be compared to earlier data and released papers. The AuthenticationService will validate the user's age and voting eligibility. It will also determine whether the present ageof the user is suitable. If all of these requirements are satisfied, the BlockchainService will invoke the vote register function and produce a new address. The client will receive the answer of the DemochainFacade contract. This will be accomplished using a customised mechanism involving the usage of a public key and an encrypted address. The clientwill then issue an API request. This approach, too, is encrypted using the server's key. The API is the most advanced that DemochainFacade can utilise. After receiving the request, it will transmit it to CryptoService for extraction and decryption. The BlockchainService will then connect to the smart contract. The key benefit of having a frontend application is that it allows people to engage with Demochain without first going via the smart contract. Technically, the application is built with React.This is the path we chose since it provides a lot of freedom, is easy to create and adjust, is incredibly versatile, and has all of the traits we needed to build what we desired. Because the target populationis so diverse, the entire programme was created to be extremely basic while also being functional in order to avoid overcomplicating the displays. It was also intended to be basic yet intuitive. The first screen is simple; it features a navigation bar with the application's logo and title, a log button in the upper right corner, and three cards with photographs and extensive information about the application's capabilities, benefits, and usage. To access the camera,the user must first enter the application's

login section. This procedure is required at this time since it will allow the user to examine the election information. After launching the camera, the user will be requested to snap another imageof his card ID so that it may be scanned. This information will be transmitted to Amazon S3 for processing to guarantee the security of the user's data. To handle data transmission to end users, an internal method will be employed. If theauthentication procedure is successful, an object containing the individual's information will be delivered to the backend. If the user does not give all of the needed information, an error message will be presented. Depending on the user's identification, the programme will behave in one of two ways. If the user is a registered voter, the first choice allows him to observe the election results, while the second allows him to handle the various options. Following the selection of an option, the user will be told at the bottom of the screen that a voting button has been triggered. An HTTP request willThe data should subsequently be sent to the backend for storage. The results page will provide a list of voting alternatives as well as different data about the registered voters.

6.APPLICATIONUSED: METAMASK, TRUFFLE-GANACHE

A. MetaMask: A software wallet that allows users to communicate with the Ethereum network via a browser extensionor a mobile app. It enables them to keep their Ethereum cash safe and to access decentralised apps.

B. Truffle and Ganache: Truffle is a framework that was utilised during the prototype development phase. It was valuable because it could operate as a package manager, but it also had built-in capability for compiling Solidity codeand distributing it to a blockchain. Truffle supplied three commands: truffle build, truffle migrate, and truffle test, which were used to create the contracts, deploy them on the network's blockchain, and test them. Ganache was used on a local PC to imitate the Ethereum blockchain. It was offered in two flavours: GUI and CLI.

Implementation: The Smart Contracts have been compiled and are linked to a MetaMask account. It is ready for deployment. The smart contracts are being implemented in Ganache Personal Ethereum Blockchain Network.The voteris now ready to vote on the candidates that have been nominated. When a voter casts a ballot for one of the candidates,the vote is logged on the network. If the person tries to vote again. Because Smart Contracts verify the complete transaction, it will be refused automatically.

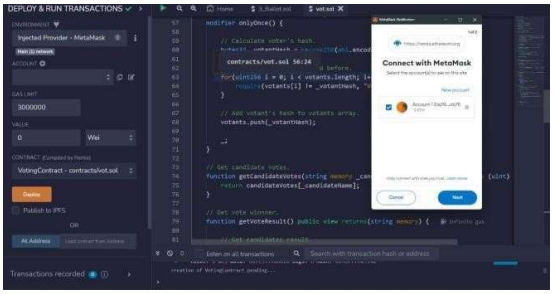

Fig 6. Connection with Metamask.

Fig 7. TRUFFLE SUITE: Inserting Available Candidates.

When a voter votes, the smart contract may automatically check the person's identification and guarantee that they areentitled to vote. This can be accomplished through a variety of means, such as biometric verification or verifying against voter registration. Once the vote is cast, the smart contract can ensure that it is securely and tamper-proof recorded on the blockchain. The smart contract may also count the votes and deliver a final total that is publicly accessible to all stakeholders.

Fig 8. Voter successfully voted.

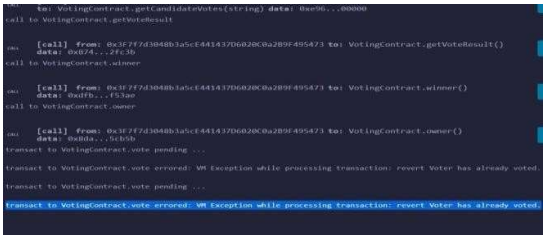

Fig 9. voters unsuccessfully voted because they tried to vote again with the same token.

In addition to evaluating the voting process, smart contracts can also enforce rules and regulations related to the votingprocess. For example, the smart contract can ensure that voters only cast one vote and that the vote is cast within a specified timeframe. This can help to prevent fraud and ensure the integrity of the voting process. Overall, smart contracts can provide a transparent and secure way to evaluate the voting process in a blockchain-based voting system,helping to ensure that the results are accurate and trustworthy.

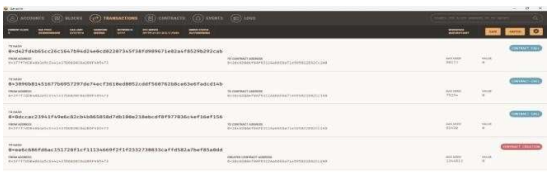

Fig 10. Transactions are recorded in Ganache.

Conclusion: There are various advantages to electronic voting systems over paper voting systems, such as their potential to boost efficiency and reduce mistakes. Several efforts have been developed to construct a blockchain-based e-voting system. This paper investigates an attempt to develop an efficient e-voting system that integrates blockchain's cryptography and transparency underpinnings. The proposed solution was carefully examined and constructed with Multichain, demonstrating its ability to satisfy the most essential needs of an e-voting system. The next research will concentrate on enhancing the blockchain's resilience against double-spending. Despite blockchain technology's effectiveness in detecting changes in transactions, we are currently investigating the prospect of developing a more secure and verifiable e-voting system. One of the most critical aspectsWe will concentrate on developing a model thatcan give a dependable and trustworthy provenance for the e-voting system. This is being developed as an additional provenance layer to complement the existing blockchain-based provenance layer.

REFERENCE:

1. ZarifKhudyakov; SuhrobBozorov;Dilshoda Ourbonalieva.”Blockchain Based E-VotingSystem: Open Issues and Challenges” pp-2021.

2. Abhishek Parmar; Sagar Gada; Trunesh Loke; Yash Jain; Sujata Pathak; Sonali Patil.”Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP”.pp-2021.

3. H.Jayasuriya;D.Bandara;N.Hemachandra;N.Kuruwitaarachchi;S.Kahandawala.“Integrity Assured DigitalVoting System by using Blockchain as the Technology”pp-2022.

4. G.Pranitha;T.Rukmini;T.N.Shankar;Basant Sah;Naween Kumar;Sasmita Padhy.”Utilization of Blockchainin E-Voting System”.pp-2022.

5. Samika Kashyap;A Jeyasekar “A Competent and Accurate BlockChain based E-VotingSystem on LiquidDemocracy”pp-2020.

6. Muhammad Shoaib Farooq;Usman Iftikhar;Adel Khelifi.”A Framework to Make Voting System TransparentUsing Blockchain Technology”pp-2022.

7. Md Jobair Hossain Faruk;Mazharul Islam;Fazlul Alam;Hossain Shahriar;Akond Rahman.”Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework”pp-2022.

8. M. Ramalingam;D. Saranya;R. ShankarRam.”An Efficient and Effective Blockchain-based Data Aggregationfor VotingSystem”pp-2021.

9. Kelechi L. Ohammah;Sadiq Thomas;Ali Obadiah;Sadiq Mohammed;Yusuf Sahabi Lolo“A Survey on ElectronicVoting On Blockchain” pp-2022

10. Divya Rathore;Virender Ranga “Secure Remote E-Voting using Blockchain”pp-2021

11. Riya Widayanti;Qurotul Aini;Hendriyati Haryani;Ninda Lutfiani;Dwi Apriliasari” Decentralized Electronic VoteBased on Blockchain P2P”pp-2021.

12. Syada Tasmia Alvi;Linta Islam;Tamanna Yesmin Rashme;Mohammed Nasir Uddin “BSEVOTING: A Conceptual Framework to Develop Electronic VotingSystem using

Sidechain"pp-2021.
13. Truc Nguyen;My T. Thai" zVote: A Blockchain-based Privacy-preserving Platform for Remote E-voting"pp-2022.
14. Saurabh Singh;Alisha Singh;Shivam Verma;Rajendra Kumar Dwivedi "Designing a Blockchain-EnabledMethodology for Secure Online VotingSystem"pp-2023.
15. Maria-Victoria Vladucu;Ziqian Dong;Jorge Medina;Roberto Rojas-Cessa"E-Voting Meets Blockchain: ASurvey"pp-2023.
16. Ehab Zaghloul;Tongtong Li;Jian Ren"d-BAME: Distributed Blockchain-Based Anonymous MobileElectronic Voting"pp-2021
17. Yang Yang;Zhangshuang Guan;Zhiguo Wan;Jian Weng;Hwee Hwa Pang;Robert H. Deng"PriScore: Blockchain- Based Self-Tallying Election System Supporting Score Voting"pp-2021
18. Aju Chhabria;Ashish Bablani;Sahil Daryani;Himani S Deshpande"Online Voting System usingBlockchain"pp2021.
19. Uzma Jafar;Mohd Juzaiddin Ab Aziz;Zarina Shukur;Hafiz Adnan Hussain."A Cost-efficient and ScalableFramework for E-Voting System based on Ethereum Blockchain"pp-2022.
20. BhartiSharma;KanikaMaheshwari;DharamveerKumar;Anvesa Jaiswal"Mobile Friendly Fully DecentralizedVoting System using Blockchain Technology and IPFS"pp-2021.
21. Lakshmi Priya K.;M.Naveen Kumar Reddy;L. Maruthi Manohar Reddy"An Integrated and Robust EvotingApplication Using Private Blockchain"pp-2020.
22. Julio César Perez Carcia;Abderrahim Benslimane;Samia Boutalbi"Blockchain-based system for e-voting usingBlind Signature Protocol"pp-2022.
23. Majd Soud;Sigurður Helgason;Gísli Hjálmtýsson;Mohammad Hamdaqa"TrustVote: On Elections We Trust withDistributed Ledgers and Smart Contracts"pp-2022.
24. More Priti Jagjivan;Jagdale Prajakta Shrikant;Jaiswal Nisha Vijay;Kale Rucha Pradeep"Secure Digital Votingsystem based on Aadhaar Authentication by using Blockchain Technology"pp-2021.
25. Bogomil Alexandrov;Eugenia Kovatcheva"Securing Nationwide Elections Through Blockchain Ledger, UtilisingEncryption Hardware"pp-2021.