IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Efficient and Secure E-Voting System Using Blockchain Technology

[1]Dr. Preethi S, [2]Dr.Bharani B R, [3]Prof. Vijayalakshmi R Y, [4]Dr.Manjunatha S

[1,2]Associate Professor, [3]Assistant Professor, [4]Associate Professor
[1,2,3]Information Science and Engineering, [4]Computer Science and Engineering
[1,2,3,4]Cambridge Institute of Technology, Bangalore, India.

Abstract— E-voting systems have been developed in recent years to improve the efficiency, security, and transparency of voting processes. However, these systems face challenges such as security threats, the possibility of vote manipulation, and issues related to voter privacy. Blockchain technology, on the other hand, has emerged as a potential solution to these challenges. Blockchain-based e-voting systems provide tamper-proof, secure, and transparent voting processes, making it difficult for attackers to alter or manipulate voting data. Additionally, blockchain-based e-voting systems ensure voter privacy by enabling voters to cast their votes anonymously while still ensuring that only authorized individuals can access the voting data. In a blockchain-based e-voting system, each vote is recorded as a block on a distributed ledger, making the voting process immutable and transparent. Smart contracts can be used to automate the voting process, ensuring that only authorized individuals can participate and that the results are accurately recorded and transparently reported. So, this implies, a blockchain-based e-voting system provides an efficient, secure, and transparent voting process, ensuring that every vote is accurately counted and that the results reflect the true will of the voters**.**

Keywords— **Blockchain, tamper-proof, secure, transparent, privacy**

INTRODUCTION

E-voting systems using blockchain technology offer a secure and transparent way to conduct elections. In a blockchain-based e-voting system, each vote is recorded as a transaction on the blockchain, making it immutable and resistant to tampering. The voting process begins with voter registration, where eligible voters are authenticated and provided with unique digital identities. This identity is used to cast a vote on the blockchain. The voter can cast their vote anonymously, ensuring privacy while still ensuring that only authorized individuals can access the voting data. Smart contracts are used to automate the voting process, ensuring that only eligible voters can participate and that the rules of the election are enforced. Smart contracts also ensure that the results of the election are accurately recorded and transparently reported. Blockchain-based e-voting systems offer several advantages over traditional voting systems. Firstly, they are more secure, as the blockchain is resistant to tampering and hacking. Secondly, they offer greater transparency, as every transaction is recorded on the blockchain and is visible to all participants in the network. This ensures that the election results are accurate and that there is no possibility of fraud or manipulation. Additionally, blockchain-based e-voting systems can improve voter turnout and accessibility, as voters can cast their votes from anywhere in the world using a secure, user-friendly interface. This reduces the barriers to voting and ensures that every vote count. E-voting systems using blockchain technology offer a secure, transparent, and efficient way to conduct elections. With the potential to increase voter turnout, reduce costs, and improve the reliability of the voting process, blockchain-based e-voting systems represent a significant advancement in the field of voting technology. Blockchain is a distributed ledger technology that allows transactions to be recorded in a transparent, tamper-proof, and decentralized manner. Each block in the blockchain contains a cryptographic hash of the previous block, ensuring that the entire ledger is immutable and resistant to any attempts at tampering. This technology is particularly useful in the context of voting, where transparency and immutability are essential. In a blockchain-based e-voting system, each vote is recorded as a transaction on the blockchain. Voters can cast their votes using a secure, user-friendly interface that ensures the privacy of their votes. The use of smart contracts allows for the automation of the voting process, ensuring that the rules of the election are enforced and that the results are accurately recorded and reported. Blockchain-based e-voting systems offer numerous benefits, including increased security, privacy, and transparency. By using blockchain technology, e-voting systems can mitigate the risks of fraud, manipulation, and hacking. Additionally, blockchain-based e-voting systems provide transparency and accountability, allowing voters to verify that their votes have been counted correctly and that the election results are accurate. Therefore, blockchain-based e-voting systems represent a significant advancement in the field of voting technology, offering a secure, transparent, and efficient way to conduct elections.

LITERATURE SURVEY

Elections form the rock of the largest democracy in the world. The methodology of election follows through universal adult suffrage, whereby every citizen over 18 years of age is eligible to vote in the eyes of constitution. Voting takes place in single member constituencies and on categorical ballot. With the merits also comes the demerits that is where a maximum section of society around the world do not trust their election system which is major concern for the democracy. Even the world's largest democracies suffer from a flawed electoral system. Disproportionality, manipulation, and polling booth capturing are the major issues in the current voting system. In this document, we are investigating the problems in the election voting systems and trying to propose the E-voting model which can resolve these issues. Also, this article aims at its best to evaluate the application and use of blockchain as service to implement distributed electronic voting systems. The section of paper will highlight few popular blockchain frameworks that offer blockchain as a service and associated electronic E-voting system which is based on blockchain that addresses all limitations respectively, it also preserves participant's anonymity while still being open to public inspection [1]. According to the IAS Parliament document, it has highlighted about the major problem in voting security where in the EVMs fail on all three pillars as established by a definitive judgement of the German Constitutional court in 2009. Other nations such as Netherlands and Ireland have also abandoned EVMs. The study found that this old voting equipment is not only more prone to failures and crashes but is also notoriously easy to hack and tamper with [2]. Blockchain is a decentralized ledger system which is built on a distributed network consisting of several interconnected nodes. These modes have transition records that are recognized by the blockchain. The blockchain include public chain, alliance chain, and private chain. Through this approach the method ensures fairness and transparency in the election process and provides fairness in the election results. In this paper, we are going to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments [3]. In this study by IEEE Access, Rivets et al presented his first concept of ring signature in the year 2001. Different from the group signature, there is no manager in the ring signature, the members in the ring need not be predefined and randomly composed. And the verifier knows the group of the signer but cannot actually determine who is the concrete signer. By introducing the above two methods, even if the data on the chain is completely open, the identity of both parties in the transaction fails to be disclosed. This paper implements anonymity of voter by using of the certificate less ring signature scheme for the blockchain [4]. As an important method of making democratic decisions, voting has always been a topic of social and economic concern. Compared with traditional methods, e-voting is widely used in various scenarios due to convenience and low cost. However, the proposed system failed due to excessive authority and tampered information. Blockchain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation [5]. This research discusses the recording of voting result using blockchain algorithms from every place of election. Unlike Bitcoin with its Proof of Work, this thesis proposed a method based on a predetermined turn on the system for each node in the built of blockchain. The use of the sequence proposed in the blockchain creation process in this system considers that in an electoral system not required for mining as in the Bitcoin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation [6]. Blockchain and other DLTs have evolved significantly in the last years and their use has been suggested for numerous applications due to transparency, accountability and redundancy. Cryptographic techniques are employed to ensure the security of voting systems in order to increase its wide adoption. However, in such electronic voting systems, the public bulletin board that is hosted by the third party for publishing and auditing the voting results should be trusted by all participants. Recently a number of blockchain-based solutions have been proposed to address this issue. However, these systems are impractical to use due to the limitations on the voter and candidate numbers supported, and their security framework, which highly depends on the underlying blockchain protocol and suffers from potential attacks [7]. To deal with two aforementioned issues, we propose a practical platform-independent secure and verifiable voting system that can be deployed on any blockchain that supports an execution of a smart contract. Verifiability is inherently provided by the underlying blockchain platform, whereas cryptographic techniques like Paillier encryption, proof-of-knowledge, and linkable ring signature are employed to provide a framework for system security and user-privacy that are independent from the security and privacy features of the blockchain platform. We analyse the correctness of our proposed voting system. We employ Hyper ledger Fabric to deploy our voting system and analyse the performance of our deployed scheme numerically [8]. Identification of need is a process of analysing what and how an end-user would expect a product to perform after edifice phase at production level. There're also nontechnical needs of an end-user or a business client which reflects the users' perception of the product and not the actual technical workaround, but they are closely related to the technical need at times. By applying the needs identification system, the organization helps to ensure the proper allocation of assets to different project within the organization [9]. Identifying of issues is the most important phase during the project that can save the organization significant amounts of time and money. Problem analysis is one of the most critical stages of project planning because this stage helps to guide all subsequent analysis and decision-making. If the project does not advance past this stage with solutions that the organization can implement, the project should not go forward in its current form. The needs for a project are identified after the organization makes observations about the project [10]. Observations are often subjective and therefore someone with expertise about the proposed project should help to make observations. A good observer can identify the needs of the project by answering key questions about the project. If the observations take into consideration the project itself and the outcome of the project, the observations should meet all of the needs of the project [11]. Observation and gathering information represent two processes. Observations highlight what is needed. On the other hand, gathering information highlights the processes needed to execute the proposed project. Both observations and the actual gathering of information should include comments from the group that ultimately will benefit from the completed project. Once the organization has analysed the needs and identified the objectives, the organization needs to allocate funds to capitalize the project [12].

By successfully identifying the needs, an organization can begin to allocate resources to pay for the project. Additionally, a business needs to consider the potential future cash flow of the project. This allows the business to analyse potential cost savings to minimize

costs and maximize the efficiency of the project [13]. The primary purpose of preliminary investigation is to identify the problem. First the need for the new and improved system is established. Only after recognising the need it is possible to perform further analysis after comparing the proposed system. At this stage we need to understand the problem and opportunities, study the existing systems and find out there are many areas where we integrate with technologies to create systems better than the existing ones. It was analysed that these proposed systems could be developed with data in mind and could provide feasible solutions [14]. The biggest challenge in this project was to integrate the existing online voting system with blockchain structure. But on further development levels we encountered various unit level problems such as the model for the Election Commission to create votes and store the necessary details of candidates along with the election details. On the later part of this document, we have come up the features which can be added to our software to make it better than the initial deployment [15].

OBJECTIVE

The objective of e-voting systems using blockchain technology is to provide a secure, transparent, and tamper-proof method for conducting elections. By leveraging the features of blockchain technology such as decentralization, immutability, and transparency, e-voting systems can help ensure that votes are counted accurately and that the integrity of the election is maintained.

With a blockchain-based e-voting system, voters can cast their votes securely and anonymously from anywhere, using their digital identity to authenticate themselves. The votes are then recorded on a decentralized blockchain ledger, which is distributed among a network of nodes. This ensures that no single entity or individual can manipulate the vote count, as the blockchain ledger is immutable and transparent.

Furthermore, e-voting systems using blockchain technology can help increase voter turnout by making it more convenient and accessible for voters to participate in the election process. They can also reduce the cost and time associated with traditional paper-based voting systems, as well as minimize the risks of human error and fraud.

To address the challenges, e-voting systems using blockchain technology aim to provide a more secure, transparent, and efficient method for conducting elections. Specifically, the objectives of such systems can be broken down as follows:

Security: E-voting systems using blockchain technology aim to provide a high level of security for the voting process. By using cryptographic techniques, digital signatures, and encryption, these systems can help ensure that votes are counted accurately and that the integrity of the election is maintained. The decentralized nature of blockchain technology also helps to prevent any one individual or entity from controlling the vote count, as the ledger is distributed among a network of nodes.

Transparency: One of the key features of blockchain technology is its transparency. E-voting systems using blockchain technology aim to leverage this feature to provide greater transparency in the voting process. By using a blockchain ledger, all votes are recorded in a tamper-proof and immutable manner, and can be accessed by anyone with the appropriate permissions. This can help to increase trust in the voting process and ensure that the election results are accurate and fair.

Accessibility: E-voting systems using blockchain technology aim to make the voting process more accessible to a wider range of people. By allowing voters to cast their votes digitally from anywhere, these systems can help to overcome barriers such as distance, mobility, and disability. They can also reduce the time and cost associated with traditional paper-based voting systems, as well as minimizes the risks of human error and fraud.

Efficiency: E-voting systems using blockchain technology aim to improve the efficiency of the voting process. By automating many of the tasks associated with traditional paper-based voting systems, these systems can reduce the time and cost of conducting elections. They can also reduce the risk of errors and inconsistencies, as well as enable faster and more accurate vote counting.

Overall, the objective of e-voting systems using blockchain technology is to provide a more secure, transparent, accessible, and efficient method for conducting elections. By addressing some of the longstanding challenges associated with traditional paper-based voting systems, these systems can help to enhance the integrity and legitimacy of the election process and increase trust in democratic institutions.

METHODOLOGY

Blockchain-based electronic voting systems can be implemented in a variety of ways, each with its own advantages and features. Using a permissioned blockchain is one strategy, which restricts access to the network to approved players who must adhere to particular rules and regulations. In private elections organized by businesses, governments, or political parties, when trust and accountability are crucial, this can be helpful.

Another strategy is to employ a decentralized blockchain, in which all nodes validate transactions and keep the ledger and there is no central authority in charge of the network. In public elections, when it is crucial to maintain transparency and thwart fraud, this strategy can be employed.

A third choice that incorporates the advantages of both permissioned and decentralized blockchain is a hybrid blockchain. To strike a balance between security, openness, and accessibility, some nodes are permitted to validate transactions and maintain the ledger, while others are accessible to anyone.

Another option that can be applied to blockchain-based electronic voting systems is smart contracts. The voting process can be automated using these self-executing computer programs, guaranteeing that only allowed voters can cast ballots and that votes are reliably tabulated. Additionally, they can be used to enforce particular laws and procedures, such as those that stop multiple voting, lessen the possibility of fraud and mistakes, and guarantee election process transparency.

A key element of blockchain-based electronic voting systems is digital identification. Voters can vote securely and anonymously after establishing their identity. Depending on the requirements of the election, digital identity can be established using a variety of techniques, including biometric authentication, cryptographic keys, or digital certificates. In blockchain-based electronic voting systems, audit trails are also crucial. They allow for the monitoring of all voting-related activities, including the casting and tallying of ballots. The election process can be made more transparent and accountable with the use of audit trails, which can also be used to look into any irregularities or disagreements that might occur.

In conclusion, the techniques of blockchain-based electronic voting systems seek to offer a safer, more open, accessible, and effective way to conduct elections. The election's particular needs, such as the required level of security, accessibility, and transparency, will determine the approach that is used.

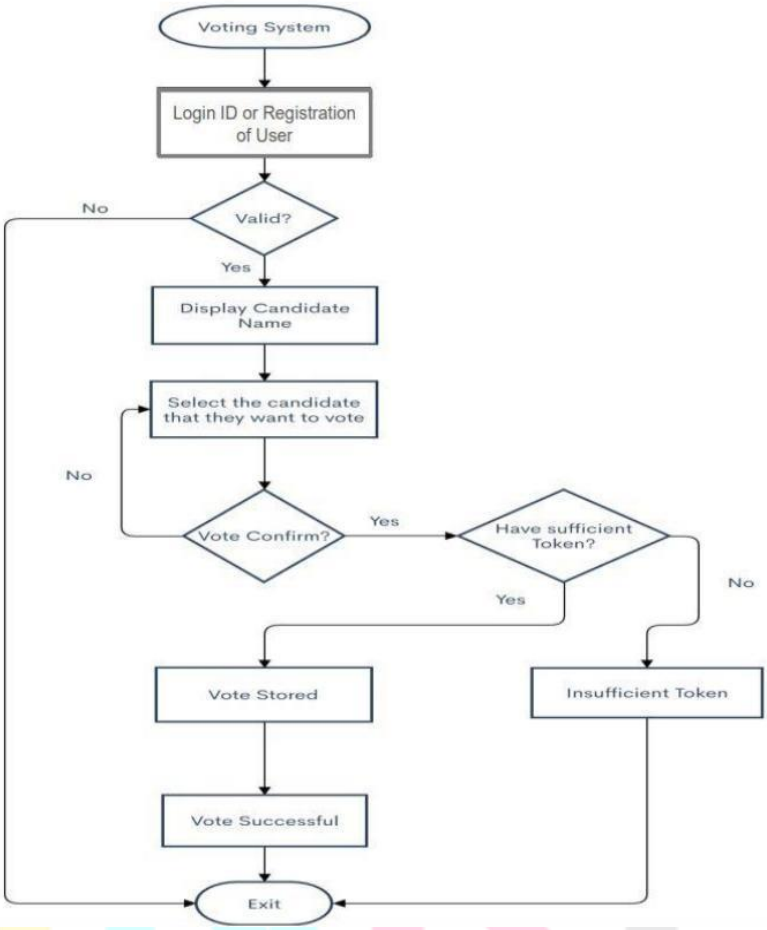

Figure.1 Flow Chart

TECHNOLOGY USED

The following technologies are typically used in e-voting systems using blockchain:

1. **Blockchain technology:** The core technology used in e-voting systems using blockchain is the blockchain itself. A blockchain is a decentralized, distributed ledger that records transactions in a tamper-proof and transparent manner. In e-voting systems, the blockchain is used to record and store voting data securely and immutably.

2. **Smart contracts:** Smart contracts are automatically-executing contracts in which the provisions of the parties' agreement are incorporated directly into the law. In e-voting systems using blockchain, smart contracts are used to automate the voting process and insure that the rules of the election are executed.

3. **Digital signatures:** Digital signatures are used to authenticate the identity of voters and ensure the integrity of voting data. Digital signatures can also be used to ensure sequestration and obscurity of choosers.

4. **Encryption:** Encryption ways can be used to cover the sequestration and security of voting data. In e-voting systems, encryption can be used to cover the identity of choosers, as well as to secure the transmission and storehouse of voting data.

5. **Public key infrastructure (PKI):** PKI is a system that uses public key cryptography to authenticate the identity of druggies and secure the transmission of data. Ine-voting systems, PKI can be used to insure the authenticity and integrity of voting data, as well as to cover the sequestration and obscurity of choosers.

6. **User interfaces:** User interfaces are used to enable voters to cast their votes securely and easily. In e-voting systems using blockchain, user interfaces can be designed to ensure that the voting process is intuitive, user-friendly, and accessible to all voters.

7. **Solidity programming:** Creating smart contracts for the Ethereum Virtual Machine requires the use of the statically compartmented programming language dependability (EVM). Reliability uses ECMAScript- suchlike syntax which makes it familiar for being web inventors; still unlike ECMAScript it has stationary typing and variadic return types.

8. **Ganache Truffle:** Ganache is actually a component of the Truffle Suite framework along with the other components, Truffle and Drizzle. Truffle serves as the development terrain, testing frame and asset channel grounded on the Ethereum Virtual Machine. On the other hand, mizzle offers a collection of different front- end libraries.

In summary, e-voting systems using blockchain generally use blockchain technology, smart contracts, digital autographs, encryption, PKI, stoner interfaces, reliability programming and ganache truffle to automate the voting process, secure the transmission and storehouse of voting data, and insure the sequestration and obscurity of choosers.

CONCLUSION

E-voting systems using blockchain technology have the eventuality to revise the way choices are conducted by furnishing a secure, transparent, and tamper- evidence voting system. The use of blockchain technology ensures that all advancing data is recorded and stored securely, and is fluently auditable, which can greatly enhance the translucency and responsibility of the election process. Also, smart contracts and digital autographs can be used to automate the voting process, reduce crimes and fraud, and insure that the election rules are executed. Despite the numerous benefits of e-voting systems using blockchain, there are still some specialized and legal challenges that need to be addressed before these systems can come extensively espoused. For illustration, issues similar as name authentication, sequestration, obscurity, scalability, and legal compliance need to be precisely considered and addressed in the design and perpetration of similar systems. Nonetheless-voting systems using blockchain have shown promising results in airman studies and trials, and they're likely to continue to attract interest and attention from governments, election authorities, and the general public in the times to come. By furnishing a secure, transparent, and effective way to conduct choices-voting systems using blockchain have the eventuality to strengthen republic, enhance name participation, and increase trust in the election process.

REFERENCES

There are some references for e-voting systems using blockchain :

[1] Mohanapriya,S., & Prakash,S.(2020). Blockchain- groundede-voting The road ahead. Journal of Ambient Intelligence and Humanized Computing, 11(3), 937- 951.
[2] Maroti,M., & Matyas,R.(2021). Blockchain- GroundedE-Voting Systems A Survey. IEEE Access, 9, 57618- 57642.
[3] Dhiman,D., & Singh,R.(2020). A Review of Blockchain- Based Electronic Voting System. International Journal of Computer Science and Information Security, 18(5), 20- 28.
[4] Saxena,P., Saraswat,R.K., & Agarwal,N.K.(2020). E-Voting using Blockchain Technology A Comprehensive Survey. IEEE Access, 8, 169738- 169764.
[5] Alam,M.S., Boutaba,R., & Chowdhury,S.S.(2020). A Blockchain- GroundedE-Voting System with Enhanced Security and sequestration Features. IEEE Deals on Network and Service Management, 17(4), 1976- 1990.
[6] Smith,C., & Orlandi,C.(2019). Blockchain Voting Systems An Overview. Computer, 52(9), 45- 51.
[7] Teixeira,M., Ferreira,R., Silva,F., & Ferreira,M.J.(2020). Blockchain- grounded voting systems a methodical literature review. Journal of Ambient Intelligence and Humanized Computing, 11(5), 1865- 1881.
[8] Li,Y., Wu,J., Guo,Y., Li,L., & Li,X.(2021). A blockchain- groundede-voting system with sequestration- conserving and fault-tolerant features. IEEE Deals on Industrial Informatics, 17(8), 5622- 5632.
[9] Etherscan. 2021. Etherscan ERC20 top commemoratives. recaptured October 15, 2021.
[10] Asem Ghaleb and Karthik Pattabiraman. 2020.
[11] NCC Group. 2021. DASP- TOP 10. recaptured January 12, 2021.
[12] Sunbeom So, Myungho Lee, Jisu Park, Heejo Lee, and Hakjoo Oh. 2020. VeriSmart A largely Precise Safety Verifier for Ethereum Smart Contracts.
[13] Chaum,D., Ryan,P.Y.A. and Schneider,P.Y.A.(2005). A practical namer- empirical election scheme, in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS' 05. Berlin, Heidelberg Springer- Verlag, 2005,pp. 118- 139.
[14] McCorry,P., Shahandashti,S.F. and Hao.F.(2017) A smart contract for boardroom voting with maximum namer sequestration in the proceedings of FC 2017.
[15] Multichain(2017) Open platform for blockchain operations. Available atwww.multichain.com last penetrated December 2017.
[16] Rosenfeld.M.(2017). Analysis of hashrate- grounded double- spending.(Online). Available http//arxiv.org/abs/1402.2009 last penetrated December 2017.
[17] Shahandashti,F.S. and Hao,F.(2016) DRE- ip A empiricalE-Voting Scheme without Tallying Authorities, the 21st European Symposium on Research in Computer Security(ESORICS), 2016.
[18] Sandler,D., Derr,K. and Wallach,D.S.(2008) Votebox A tamper-apparent, empirical electronic voting system, in Proceedings of the 17th Conference on Security Symposium, ser. SS' 08.
[19] AdidaB. and Rivest,R.L.(2006). Scratch & bounce tone- contained paper- grounded cryptographic voting, in Proceedings of the 5th ACM Factory on sequestration in Electronic Society, ser. WPES' 06.

[20] Bell,S., Benaloh,J., Byrne,M.D., Debeauvoir,D., Eakin,B., Kortum,P., McBurnett,N., Pereira,O., Stark,P.B., Wallach,D.S., Fisher,G., Montoya,J., Parker,M. and Winn,M.(2013).
[21] H. V. Patil, K. G. Rathi, and M. V. Tribhuwan, ''A study on decentralized e-voting system using blockchain technology,'' Int. Res.J.Eng.Technol, vol. 5, no. 11, pp. 48–53, 2018.
[22] Agora. (2017). Agora: Bringing Our Voting Systems Into the 21st Cen tury. [Online].
[23] R. Taş and Ö. Ö. Tanrıöver, ''A manipulation prevention model for blockchain-based E-voting systems,'' Secur. Commun. Netw., vol.2021, pp. 1–16, Apr. 2021.
[24] E. Zaghloul, T. Li, and J. Ren, ''Anonymous and coercion-resistant dis tributed electronic voting,'' in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2020, pp. 389–393.
[25] T. Dimitriou, ''Efficient, coercion-free and universally verifiable blockchain-based voting,'' Comput. Netw., vol. 174, Jun. 2020, Art. no. 107234.
[26] Dr. Preethi S, Dr. Jayanthi M G and Ms. Yashaswini S, "An Efficient Hybridization Approach for Tissue Segmentation and Classification in Brain MRI Images", International Journal of Novel Research and Development, ISSN 2456-5184, 03-03-2023.