International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN

Shrutika Gawali[1], Deepika Khadgade[2], Shrutika Kolhe[3], Nikita Vyavhare[4], Prof. Madhuri B. Babar[5]

J D College of Engineering and Management, Nagpur
Dr. Babasaheb Ambedkar Technological University, Lonere, India

---

Abstract - This design proposes the design and development of a decentralized voting system using blockchain technology and face recognition. The end is to produce a secure, transparent, and accessible voting process that ensures the integrity and delicacy of election results while icing the insulation of pickers. The system will use blockchain technology to produce a decentralized and tamper- substantiation census of votes, and face recognition technology to insure that each vote is cast by an eligible name. The design aims to contribute to the ongoing sweats to develop farther secure and accessible voting systems that enhance popular processes and cover the integrity of choices.

***Key Words*: Blockchain, Decentralized, E-voting, Voter Privacy, Face Recognition**

1. INTRODUCTION

Voting schemes have evolved from counting hands in early days to systems that include paper, punch card, mechanical switch and optical- scan ma- chines. An electronic voting system which is used presently give some characteristic different from the traditional voting fashion, and also it provides bettered features of voting system over traditional voting system analogous as delicacy, convenience, strictness, insulation, verifiably and mobility. But Electronic voting systems suffers from various downsides analogous as time- consuming, consumes large volume of paper work, no direct part for the advanced officers, damage to machines due to lack of attention, mass update does not allow stoners to contemporize and edit multitudinous item simultaneously etc. therefore, by administering a decentralized Blockchain predicated garçon terrain we can help data loss. Blockchain is a distributed census technology that allows secure and transparent record- keeping of deals across a network of computers. The technology was first introduced in 2008 by an anonymous person or group of people under the alias Satoshi Nakamoto in a white paper named" Bitcoin A Peer-to- Peer Electronic Cash System." At its core, a blockchain is a database that's maintained by a network of bumps that collectively validate and record deals in a decentralized and secure manner. SHA- 256 a fixed- size 256- bit (32- byte) hash value. It's one of the most considerably used hash functions in the world and is used in various operations, including digital signatures, word storage, and blockchain technology. SHA- 256 takes an input communication of arbitrary length and produces a fixed- size affair, which is a unique digital point of the input communication. The affair, also known as the hash value, is generated using a series of fine operations that can't be re- clued, making it nearly impossible to gain the original input communication from the hash value.

1.1 Blockchain

Blockchain is a distributed ledger technology that al-lows secure and transparent record-keeping of transactions across a network of computers. The technology was first introduced in 2008 by an anonymous person or group of people under the pseudonym Satoshi Nakamoto in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." At its core, a blockchain is a database that is main-tainted by a network of nodes that collectively validate and record transactions in a decentralized and secure manner.

1.2 SHA – 256 Algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that generates a fixed- size 256-bit (32-byte) hash value. It is one of the most widely used hash functions in the world and is used in various applications, including digital signatures, password storage, and blockchain technology.

SHA-256 takes an input message of arbitrary length and produces a fixed-size output, which is a unique digital fingerprint of the input message. The output, also known as the hash value, is generated using a series of mathematical operations that cannot be re- versed, making it practically impossible to obtain the original input message from the hash value.

2. LITERATURE SURVEY

Ehab Zaghloul focuses on voter privacy through secure multiparty computation performed by parties of differing allegiances. In the security and privacy analysis, it shows that the proposed scheme is secure against potential security threats and provides voter anonymity. The purpose of [2] study is to examine and assess current research on electronic voting system based on blockchains. The idea of blockchain and its applications are introduced first, followed

by a discussion of existing electronic Voting System. The article addresses recent blockchain based electronic voting system research. In the research paper [3] The proposed blockchain architecture shows how Blockchain using Smart contracts and hyper ledger Fabric will be utilized to handle e-voting system security concerns. The diagrams and flow charts of paper further break down into the defined proposed process intimately, which makes it a possible reality to beat the protection limitations and adoption obstacles related to the electronic legal system. [4] So further study, tells that the benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. Also, due to the encryption mechanism, it is not possible for any person to gain access to all the votes without first taking control of the entire service network.

3. PROPOSED SYSTEM:

The proposed system is the Biometric online voting system with biometric point using Aadhar card. It determines the particular name by his/ her point whether he she is a valid name or not. It allows particular name to cast the vote online.

The polling process continues until the voting time ends and modernize the database in the garçon. Biometric online voting system uses Aadhar card to recoup the complete details about the name. And the votes are stored in a blockchain garçon and viewed to the public this insure a secure terrain.

4. METHODOLOGY:

The methodology for assessing the result of a decentralized voting system using blockchain and face recognition technology would involve several ways.

1. Design and Development The first step would be to design and develop the decentralized voting system using blockchain and face recognition technology. This would involve concluding applicable blockchain technology, developing the face recognition system, and integrating both technologies to produce a secure, transparent, and accessible voting process.

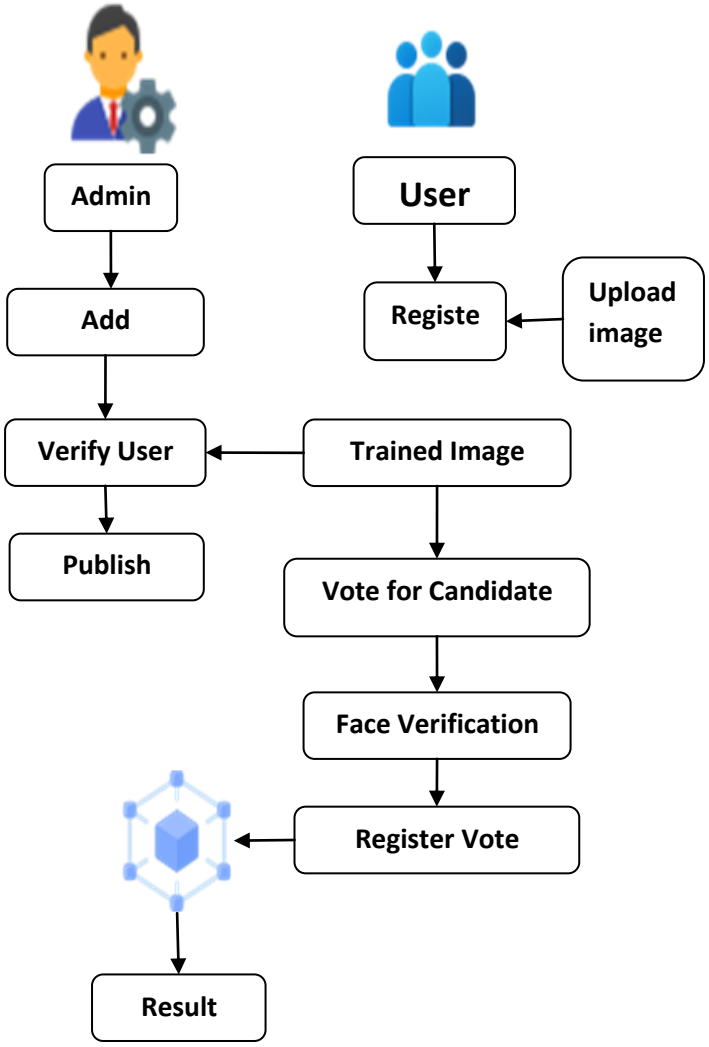
2. Testing and Evaluation The coming step would be to test the system and estimate its performance. This would involve conducting birdman tests with many pickers to ensure the system is working correctly and to identify any issues that need to be addressed. The system's performance would be estimated predicated on several factors, analogous as security, delicacy, vacuity, and insulation.

3. Data Collection and Analysis The system's performance data would be collected and anatomized to estimate the result of the decentralized voting system. The data would be anatomized using statistical and data visualization ways to identify patterns, trends, and perceptively that can help meliorate the system's performance.

4. Comparison with Traditional Voting Systems The result of the decentralized voting system would be compared with the traditional voting systems to estimate its effectiveness. The comparison would involve assaying the delicacy, security, vacuity, and cost- effectiveness of the decentralized system compared to traditional systems.

5. Feedback and improvement the final step would be to gather feedback from pickers, election officers, and other stakeholders to identify areas for improvement. The feedback would be used to upgrade the system's design and development, making it more effective, secure, and accessible.

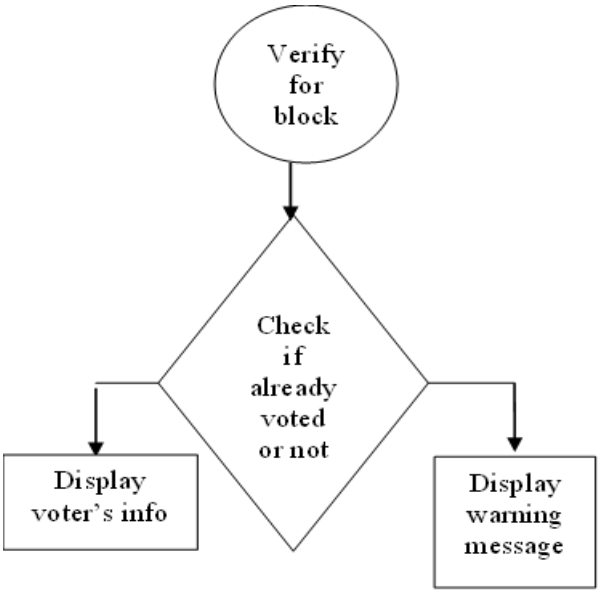
5. SYSTEM ARCHITECTURE:



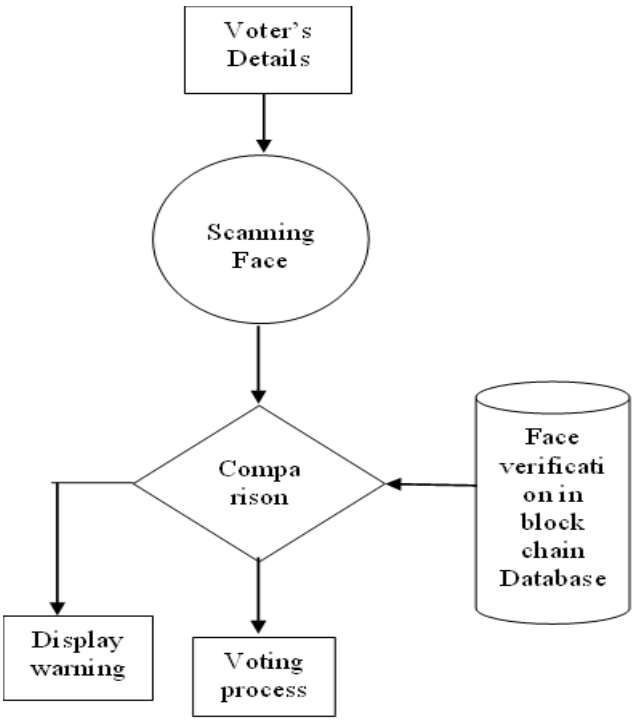
6. DATA FLOW DIAGRAM:

A Data Flow Diagram (DFD) is a graphical **representation of the "flow" of data through an** information system, modelling its aspects. It is a preliminary step used to create an overview of the system which can later be elaborated DFDs can also be used for visualization of data processing.

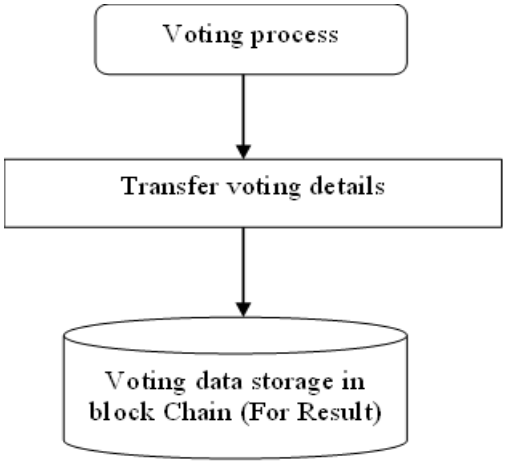
Level 0:



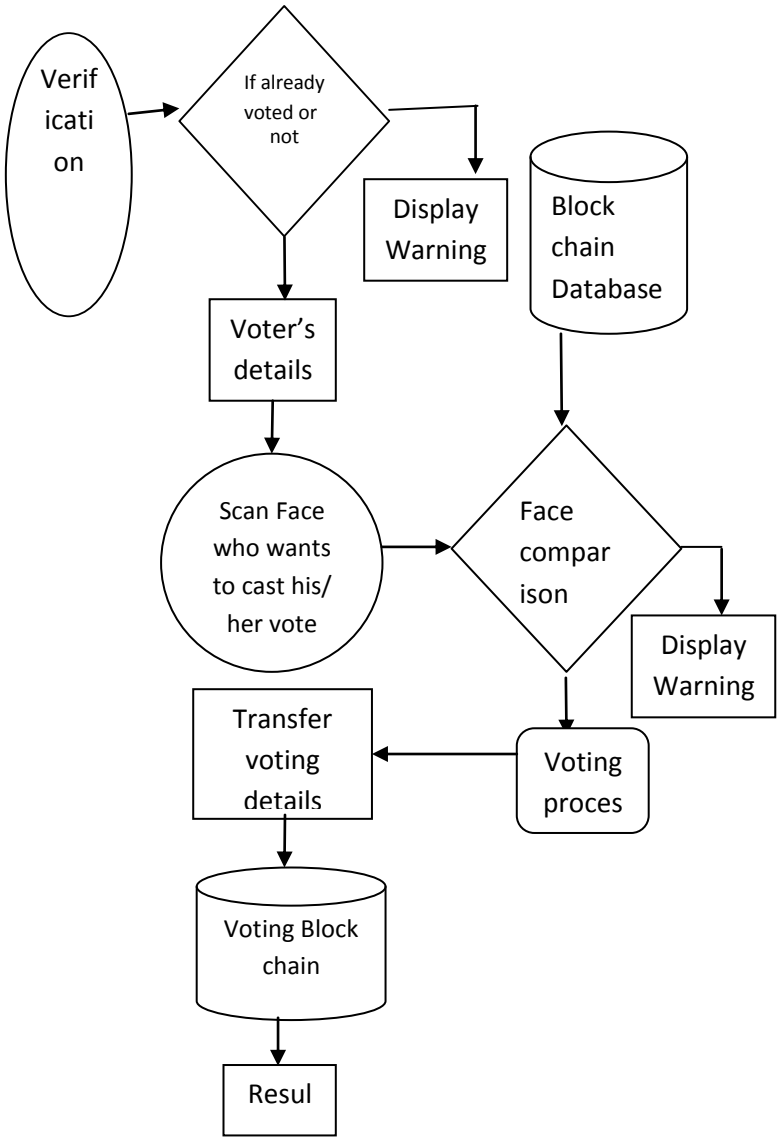
Level 1:



Level 2:



Level 3:



7. IMPLEMENTATION

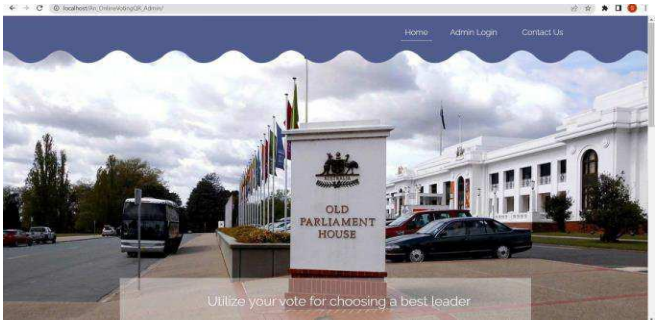


Fig. 7.1 User Interface

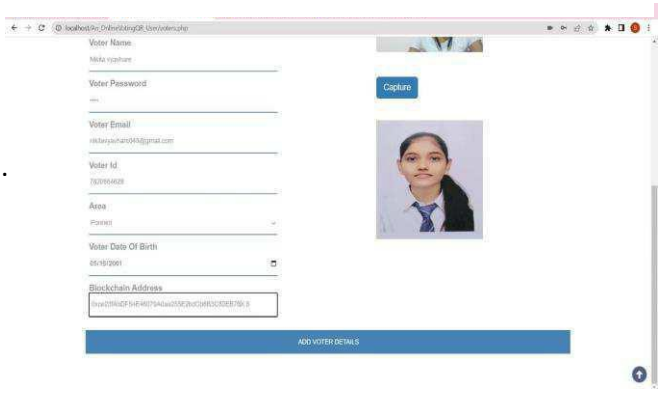


Fig. 7.2 User Registration

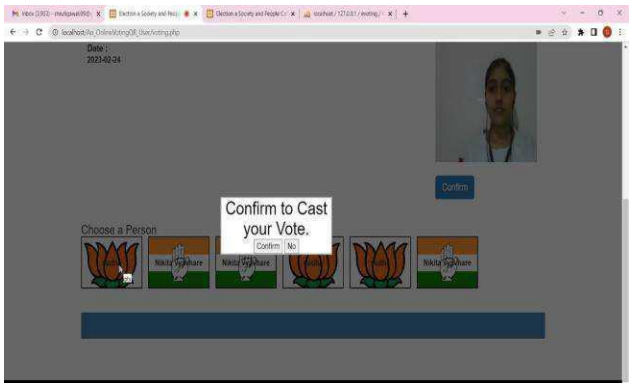


Fig. 7.3 Vote Casting

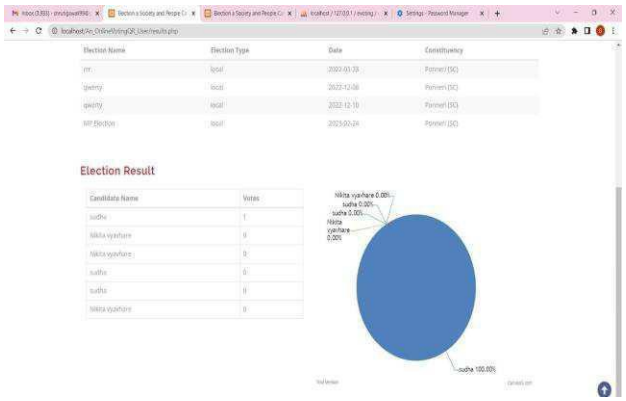


Fig. 7.4 Result

8. DISCUSSION

Decentralized voting systems using blockchain and face recognition technology have the eventuality to revise the voting process by furnishing a more secure, transparent, and accessible voting process. The use of blockchain technology provides a tamper-evidence and transparent tally that ensures accurate and auditable results while guarding against fraud, manipulation, and hacking. Face recognition technology, on the other hand, can give an accessible and accessible way to corroborate the identity of choosers while guarding their sequestration. Still, the perpetration of decentralized advancing systems using blockchain and face recognition technology isn't without its challenges. One major concern is scalability, as the technology may not be suitable to handle the high volume of choosers that are present in large-scale choices. Also, the use of face recognition technology raises enterprises about sequestration and the eventuality for abuse of particular data. Thus, there's a need for sequestration- conserving ways that ensure the obscurity of choosers and cover their particular information. Likewise, standardized protocols and regulations are demanded to ensure interoperability and wide relinquishment of decentralized voting systems using blockchain and face recognition. Eventually, there's a need for further exploration on the impact of the technology on name get and participation, as well as the usability and availability of the technology for all eligible choosers. Overall, decentralized voting systems using blockchain and face recognition technology have the eventuality to significantly ameliorate the voting process by furnishing a more secure, transparent, and accessible system. Still, the challenges associated with enforcing the technology must be announcement- dressed to ensure its successful relinquishment and integration with being voting systems.

9. RESULT:

The result of enforcing a decentralized voting system using blockchain and face recognition technology would be a more secure, transparent, and accessible voting process. The use of blockchain technology would ensure the integrity of the voting process by furnishing a tamper-evidence and auditable tally, while face recognition technology would give an accessible and accessible way to corroborate the identity of choosers while guarding their sequestration. By enforcing a decentralized voting system using blockchain and face recognition, it would be possible to help fraud, manipulation, and hacking in the voting process. This would increase the delicacy and translucency of election results, thereby promoting trust in the voting process and the popular system as a whole. Also, the use of face recognition technology would make the voting process more accessible to all eligible choosers, including those with disabilities or limited access to technology. The technology could also reduce the need for physical polling stations, making it more accessible for choosers to cast their vote from anywhere at any time. Still, the perpetration of a decentralized advancing system using blockchain and face recognition technology

isn't without its challenges. Technical, cost, and scalability enterprises must be addressed to ensure the technology is a feasible and extensively espoused result for secure and accessible voting. Sequestration enterprises associated with the use of face recognition technology must also be addressed to cover the obscurity of choosers and help abuse of particular data. Overall, the result of enforcing a decentralized advancing system using blockchain and face recognition technology would be a more secure, transparent, and accessible voting process that promotes trust in the popular system and ensures accurate and fair election results.

10. SUMMARY:

A decentralized voting system using blockchain by face recognition is a promising solution for enhancing the security and transparency of the voting process. This system utilizes facial recognition technology to ensure the accuracy of a decentralized voting system using blockchain by face recognition is a promising solution for enhancing the security and transparency of the voting process. This system utilizes facial recognition technology to ensure the accuracy of voter identification, while blockchain technology provides a tamper-proof and immutable ledger of all voting transactions. The use of the SHA-256 algorithm further enhances the security and integrity of the system. Overall, this technology has the potential to increase voter participation, enhance election security, and improve the trust and legitimacy of the democratic process.

11. CONCLUSIONS

In conclusion, a decentralized voting system using blockchain by face recognition has the potential to revolutionize the voting process by providing a secure, transparent, and tamper-proof system. The integration of facial recognition technology can help fraud, to prevent fraudulent voting and ensure the accuracy of voter identification, while blockchain technology can pro-vide a decentralized and immutable ledger of all trans-actions. The use of the SHA-256 algorithm can further enhance the security and integrity of the system by creating unique digital fingerprints of voter information, votes, and blocks.

However, there are still several challenges that need to be addressed to ensure the widespread adoption of such a system, including concerns about the accuracy and bias of facial recognition technology, the need for secure and reliable hardware, and the potential for cyber-attacks on the blockchain network. Additionally, legal and regulatory frameworks will need to be developed to address issues such as voter privacy, data protection, and transparency.

Despite these challenges, a decentralized voting system using blockchain by face recognition has the potential to increase voter participation, enhance election security, and improve the overall trust and legitimacy of the democratic process. Further research and development in this area can help to overcome the remaining obstacles and bring about a new era of secure and transparent voting systems. The remaining obstacles and bring about a new era of secure and transparent voting systems.

12. REFERENCES

[1] D-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting Ehab Zaghloul, Tong-tong Li, Senior Member, IEEE, and Jian Ren, Senior Member, IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 22, NOVEMBER 15, 2021

[2] Blockchain Based Online Voting System Using RSA Algorithm Kingsle Edwin, Hepzibah Christinal and Abraham Chandy, EasyChair: Institute of Tech-nology and Sciences, Coimbatore, India February 1, 2022

[3] Securing the Electoral E-Voting System Using Blockchain Technology Taiwo Adekeye Data Science 5 and Artificial Intelligence Bournemouth University Bournemouth, United Kingdom, uploaded by Taiwo Adekeye on 13 January 2022.

[4] Secure Voting System using Blockchain Method Manav Tiwari, Utkarsh Thaokar, Sahil Sangwan, Shubham Gupta, Department of Information Technology, Sinhgad Institute of Technology, Lonavala, India. International Journal of Research in Engineering, Science and Management, Volume 5, Issue 1, January 2022.

[5] Data Management, Analytics and Innovation Pro-ceedings of ICDMAI 2019, Volume 1, Advances in Intelligent Systems and Computing Volume 1042, Series Editor: Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

[6] Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability, Shufan Zhang · Lili Wang · Hu Xiong © Springer-Verlag GmbH

[7] Using Blockchain Data Security Management for E-Voting Systems Erick Febriyanto, Triyono, Nina Rahayu, Kelvin Pangaribuan, Po Abas Sunarya The 8th International Conference on Cyber and IT Service Management (CITSM 2020) On Virtual, October 23-24, 2020

[8] ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication Mohamed Ibrahim, Kajan Ravindran, Hyon Lee, Omair Farooqui, Qusay H, Mahmoud 2021 IEEE 18th Inter-national Conference on Software Architecture Com-panion (ICSAC)

[9] Digital Voting: A Blockchain-based E-Voting Sys-tem using Biohash and Smart Contract Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam EEE Xplore Part Number: CFP20P17- ART; ISBN: 978-1-7281-5821-1

[10] Decentralized E-voting system based on Smart Contract by using Blockchain Technology Ali Mansour Al-madani, Dr. Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T. Ahmed

[11] The Future of Electronic Voting System Using Blockchain Md. Razu Ahmed, F.M. Javed Mehedi Shamrat, Md. Asraf Ali, Md. Rajib Mia, Mst. Arifa Khatun INTERNATIONAL JOURNAL OF SCIEN-TIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 02, FEBRUARY 2020 ISSN 2277-8616