Online Voting Platform Using Blockchain Technologies

Sonali Rangdale[1], Nagesh Raykar[2], Santosh Borde[3], PrashantKumbharkar[4,] Uditkumar [5]

[1]JSPMsRajashriShahuCollegeofEngineering,Pune-411033,India,
Pune-India, Sonalirangdale1278@gmail.com

[2]ShriJagdishprasadJambharmalTimbrewalaUniversity,Jhunjhunun,India
Pune-India, Nageshkraykar@gmail.com

[3]JSPMsRajashriShahuCollegeofEngineering,Pune-411033,India,
Pune-India, spraoborde@gmail.com

[4]JSPMsRajashriShahuCollegeofEngineering,Pune-411033,India,
Pune-India, Pbk.rscoe@gmail.com

[5]BML Munjal University, Gurgaon-122413,India,
Gurgaon-India, Udit.kumar.22cse@bmu.edu.in

***Abstract*:**
Developing a secure electronic voting system that preserves the privacy and fairness of current voting practices while offering the flexibility and transparency offered by electronic systems has long been a challenge. This draft article's objective is to develop a system that evaluates a block chain application for use in the deployment of dispersed electronic voting systems**..** The objective of this study offers a novel block-chain-based electronic voting system that tackles some of the drawbacks of current systems and assesses ome of thewell-knownblockchainframeworksinordertobuilda blockchain-based e-voting system. Through the explanation of a case study, specifically the election process and the deployment of a block chain-based application that enhances the security and efficiency of voting, we specifically assess the potential of distributed ledger technology. The results of the system shows significant improvement in security as compare to traditional voting system.

Keywords*: *Blockchain, Voting, Bitcoin, IoT;

(Article history: Received: Oct 31,2023 and accepted Jan, 31,2024)

I. INTRODUCTION

In today's society, blockchain technology is becoming popular. The blockchain voting system's finest example is Bitcoin. In supply chain management systems, it is employed. Payroll, healthcare, business, Internet of Things, voting systems, etc. The voting mechanism in use today is not reliable or secure due to the numerous attacks that occur, including DDoS attacks, polling attacks, and virus capture attacks. In addition, it is a labor-intensive procedure that takes a long time and involves a lot of paperwork. Several drawbacks include: The hazards of data loss and vote rigging, human engagement in COVID-19, Less time-consuming and ecologically sustainable, Even elderly individuals find it comforting.[1] The price is steep. When a voter presses the button on the electronic voting machine (EVM) representing their preferred party during an election. What assurance does the voting machine provide? How to find out if your vote has been counted successfully. Ballot sheets are also used, in addition to EVM. There is no way to ensure that ballots will be counted or that frauds will occur when voting via paper ballot. The central government guarantees this to us; in other words, in order for our votes to be correctly counted, we essentially have to blindly trust the Election Commission (EC) to function as intended.[2] But consider the scenario in which we could have ensured this on our own without the help of the Election Commission or any other third party. If we could verify that our vote has been counted without needing to rely on third parties, that would be quite goodAre you aware that blockchain can be used to create such a system? The best illustration of blockchain technology is Bitcoin. Voting systems can be completely altered, according to experts, by blockchain technology. In what way is this feasible? How is this blockchain technology implemented? In [4]The fundamental idea behind blockchain is the decentralised data storage method. With blockchain technology, data cannot be altered or the system controlled. Using RBI as an example The Reserve Bank of India prints 500 rupee notes. RBI promises that it will always be 500 and never 501 or 502. Even the note states that the RBI guarantees it, therefore in essence; the RBI is the central authority in charge of all Indian rupee notes that are in circulation

worldwide. RBI has the ability to alter the value. The RBI has the power to alter the amount of notes produced, while decentralised currencies like Bitcoin do not.[3]

I.Literature survey

Bitcoin is not governed by any Central Agencies or authorities. Because Bitcoin is likewise decentralised, it is feasible. Bitcoin is truly decentralised thanks to blockchain technology. Each brick is unique in its fingerprint. Thirdly, every block in this series retains the fingerprint data of the blocks that came before it. We refer to this as blockchain. Voting is a more efficient and economical method. This block and the block behind it will each have unique fingerprints. Any further information you may add comes next [4, 5, 6]. It'll be stored in a block. It'll be kept in blocks. All blocks are connected to one another in this way. The most distinctive feature of this is that the fingerprint, or hash, of the block will change if you try to alter the data in any block or if you want to modify any of the data. The blockchain will automatically cease to exist if the hash value of one block changes, as will the hash values of the next and subsequent blocks. As a result, data in a blockchain cannot be altered or compromised. Once a block is created and added to the blockchain, it cannot be removed. The decentralisation of blockchain is the second main factor contributing to its security. Blockchain data is kept on a computer network [7]. One copy of this blockchain will be stored on every machine participating in the blockchain worldwide. It is jointly governed and operated by a network of computers rather than by a single central authority. Those who allow the blockchain to run on their laptops or mobile devices, as well as those who are linked via PCs or cellphones. We refer to them as Nodes. Miners make up a portion of these Nodes. Miners are responsible for verifying newly added data to the blockchain [8]. Is the data being added by this person correctly? If there is an effort to tamper. Each and every miner attests to this. This data has been added to the blockchain and can be read by any computer that is connected to the system. [/9]. Consider them to be a password and email address. You can access your Gmail account by entering your Gmail ID and password throughout the login process. With blockchain, it works similarly. However, sharing your public address—rather than your private key—with others when you store something implies sharing your email address. However, nothing about the individual behind the public address—name, age, or address—will be revealed. There will be privacy preservation. [5]

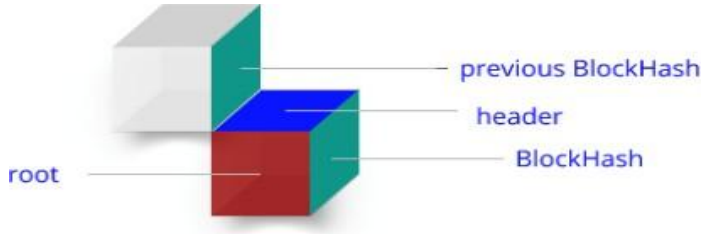

Fig1:Basic Structure of Blockchain

II. PRAPOSED WORKING BLOCK CHAIN BASED VOTING SYSTEM

Hence diagram given below explains how the blockchain voting works.

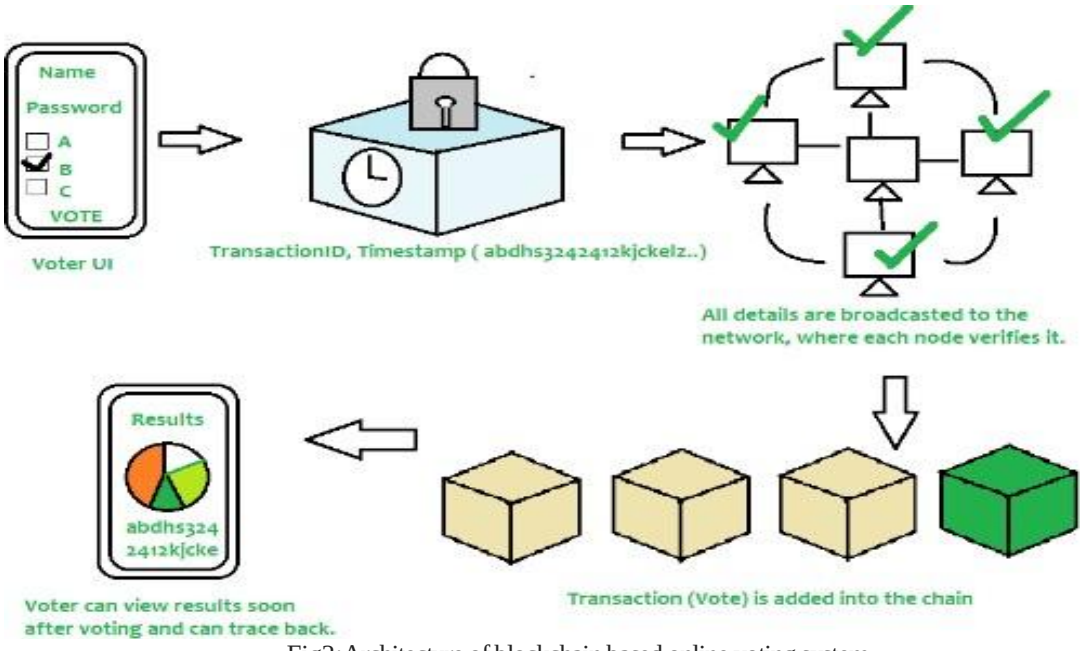

Fig2:Architecture of blockchain based online voting system

The voter must submit their credentials in order to cast a ballot, as seen in the diagram above. Once encrypted, every piece of data is kept in a transactional database. Every node in the network receives a broadcast of this transaction, which is subsequently confirmed [10]. A transaction is added to the chain and saved in a block if the network authorises it. Keep in mind that once a block is added to the chain, it cannot be removed and remains there indefinitely. Now, users can view the outcomes and, if they'd like, track back the transaction. Since the security requirements of the present generation are not met by the voting systems in place, a system that takes advantage of the security, convenience, and trust aspects of voting must be developed.[7] Therefore, blockchain technology is used in voting systems to provide an additional degree of security, enable people to vote whenever and wherever they choose, and create ways for devices to stop it from happening. Suppose we are dealing with bitcoin and we need to move 2000 rupees from X to G. The 2000 rupees will be transferred, and a new block with X and G's public addresses will be created. Now, this will be saved by other web-connected devices like computers and mobile phones. They will document that X started the transfer to G, note the amount sent, and then confirm the transaction.. In a decentralized network, if one computer indicates that a transfer originates from X to G rather than from X to itself, the other computers recording the transaction will reject the claim due to the evident discrepancy. Consequently, the system will rely on feedback from other devices on the web to validate the transaction from X to G. For any hacker attempting fraud or alterations in the blockchain, they would require a majority stake of at least 51%. This vulnerability represents a significant drawback of blockchain voting systems. Should a hacker manage to control 51% of the computers within the network, fraudulent activities could be facilitated. However, realistically, hacking a majority of the network's computers is exceptionally challenging. Since these computers are decentralized and operate independently, compromising one does not compromise others. Each computer would need to be individually targeted and breached. In extensive blockchain networks like Bitcoin, comprising millions of globally distributed computers, the prospect of such a large-scale hack is virtually impossible. The decentralized nature of these networks ensures resilience against such attacks, as each node operates autonomously without direct interconnection. Turning to real-life applications, blockchain technology has already found utility in various sectors, including electoral processes. For instance, in Sierra Leone, blockchain was utilized during elections for voting purposes, although many experts argue against its suitability for such critical processes. Despite its robust security measures, blockchain is susceptible to personal-level attacks, especially in instances of network vulnerabilities. Consequently, discussions about implementing blockchain solutions and assessing their feasibility warrant expert deliberation. Beyond electoral processes, blockchain holds promise in diverse fields such as healthcare. By storing patient data on a blockchain, privacy can be enhanced, and access can be restricted to authorized personnel, thereby mitigating risks associated with centralized databases. Additionally, blockchain technology can facilitate trustless transactions, such as in trading scenarios where parties may lack mutual trust. Through smart contracts executed on blockchain platforms, transactions can be automated and secure, eliminating the need for intermediaries. Property management, crowdfunding, and data management are among the myriad other applications of blockchain technology. With governments increasingly relying on digital infrastructure for data storage, blockchain offers a compelling solution to enhance security and mitigate risks of data breaches. By decentralizing data storage and enabling peer verification, blockchain technology can bolster data integrity and protect sensitive information from unauthorized access. As we transition towards a decentralized future, blockchain is poised to play a pivotal role in reshaping digital ecosystems. Platforms like ARGO are striving to streamline transactions and promote widespread adoption of blockchain technology. Proponents envision blockchain as a transformative force akin to the internet, revolutionizing various facets of human society. Just as we cannot imagine life without the internet today, many believe that blockchain will soon become indispensable in our daily lives. The future holds exciting possibilities for blockchain, and its full potential is yet to be realized.

Need of Block Chain Technologies:

There are some characteristics of blockchain technology like secure, reliable, decentralize, immutable. Let’s take an example to understand blockchain voting system. Suppose you are voter in your country and you are giving vote to your favorite candidate. In case if someone tampers with microchip and divert your vote to another candidate you will never know your vote is counted or diverted to some other candidate. There is no trace back of your vote. But if you are giving vote through online voting system which is totally based on blockchain technology then your vote is stored in format of transaction and each transaction has its own id and each id is totally different from each other [10].There will be no chances of fraud. It will give you receipt of every transaction done by you. By the way this is online voting system so you can give vote anywhere from your country on specific time [18]. You don’t have to go election centre and don’t have to waste your valuable time. You can give vote on your Computer, Laptop even on Mobile and Tablets also. In Online Voting system user have to do some procedures which mentioned in following:

1) User have to done registration in specific time which is set by network administrator and information and documents submitted by user is verified by higher authorities.
2) User id and password will provide to user to their registered mobile number which is linked to PAN card number [8].
3) At time of voting user can give vote to their favorite candidate on mobile or computer.
4) User will get transaction id of their vote which is not in today’s voting system.

5) User can see each transaction on their system.

Some important concept in blockchain voting system are:

- Contract: It is program which is run on blockchain Ethereum. It is collection of code and data which is in specified address of blockchain.
- Structure: Structure is collection of different data types.
- Mapping: It stores value which is based on key. We can do iterating over mapping.
- Modifier: Modifiers can change the characteristics of function. It can check condition automatically.

Different types of voting: Elections in India are currently conducted through EVMs and postal voting. People over the age of 18 can vote for their favorite candidates. This is the greatest proof of freedom. People vote to improve their communities. India started using EVMs in elections 30 years ago. An EVM machine is a device consisting of a motherboard, processor, and softw are (also known as firmware). Preelection events are held. The Election Commission conducts a verification process and candi dates can check the working of the EVM before using it for the election. It ensures that votes are given to the correct candidate. Vote fraud. EVM tampering has occurred in many countries such as South Africa in 1994, Ukraine in 2014, and the United Sta tes in 2014. Voter tampering has occurred in the UK and the US. Voter fraud can also occur in Parliament. Online voting is a pl atform that provides the ability to vote through a website or mobile application or any device on the internet. However, there ar e security issues with online voting that is not based on blockchain technology. To ensure security, we need to encrypt data to p rotect it. We can protect this system using 256-bit encryption

III. METHODOLOGY

Voters would use their preferred personal device (i.e., desktop, laptop, smartphone, or tablet to download and install the voting application booth in order to use our blockchain voting system. After that, the voter would provide the necessary identity details to have their identity confirmed by an Identity Verifier, who would then confirm the voter's identity based on approval from the organisation holding the election beforehand. After their identity has been confirmed, the voter can request a ballot; the Registrar will then issue the appropriate ballot type. After filling out their ballot, the voter would safely deposit it into the blockchain-powered voting machine. The voter would be able to print off a confirmation of their ballot casting.The application is developed with implementation of Keccak-256 algorithm. The Keccak-256 is a cryptographic hash function that produces a 256-bit output, which is commonly used in various applications, such as digital signatures, data integrity checks, and password storage. It was developed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche in 2008 as a part of the SHA-3 competition held by the National Institute of Standards and Technology (NIST). Keccak-256 op- erates on a message of arbitrary length and produces a fixed-size output of 256 bits. It uses a sponge construction, which means that it first absorbs the message into an internal state, and then squeezes the state to produce the output. The internal state of Keccak-56 consists of a 5x5 matrix of 64-bit words, which is initialized to a fixed value at the beginning of the computation.[11] The absorption phase of Keccak-256 works by partitioning the message into blocks and XORing them with the internal state. Each block is also transformed using a nonlinear function called the Keccak-p permutation, which operates on the entire state? The permutation consists of five rounds, each of which applies a set of linear and nonlinear operations to the state. Keccak - 256 has several desirable cryptographic properties, such as resistance to differential and linear cryptanalysis, and the property of being a "one-way" function, which means that it is computationally infeasible to invert the function and recover the input message from the output hash. We can conclude that, Keccak-256 is a secure and efficient cryptographic hash function that can be used in a wide range of applications. It is resistant to various attacks and provides strong cryptographic properties that en- sure the integrity and authenticity of data.

A. Process Flow

There are many ways to introduce changes in electronic and online voting system by different methods and techniques. Some of the projects are guarantees the security, confidentiality and integrity as well at some extent. But there is need of software and hardware and some modern techniques which ensures the privacy of voter’s information. Online voting system is approach, user can vote on website or app on any electronic device like computer, mobile which uses various decryption and encryption technique which ensure privacy and security. Homomorphic encryption is transformation of data into cipher text, which can be examine used just like the original from. Homomorphic encryption is used for solving complex arithmetic problems on en-crypted data without breaking encryption of data. Using Homomorphic encryption data owner can encrypt data and send to the server. It’s major advantage it is worked on encrypted data without knowing private key. Its major disadvantage is poor per-formance due to computationally heavy application [12].

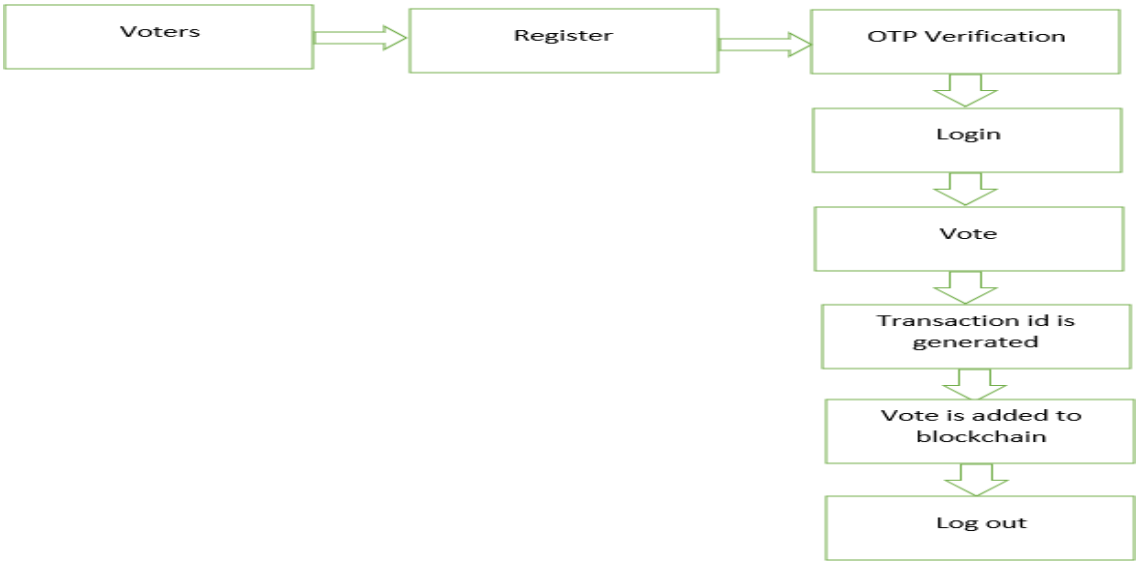

Fig 3: Process of proposed voting system

This is E-voting system is fully based on blockchain technology. In this system data has been stored in Ethereum blockchain which is decentralized and secured thus all data is not allowed at central location. The registrations of candidate and voters will be done before election period. Practically documents of voters authorized by respected department. After verifying Identity, the authorized user will approve eligible users by verifying token or coin. Voters have not a permission to give more than one vote. Voters may cast early ballots and, if permitted by the election hosting organisation, alter their vote in the days preceding the election by returning to the Follow My Vote voting booth. Voters would be able to track their ballot into the ballot box to confirm that it was cast as intended and tallied as cast, and the most recent votes submitted by each voter would be deemed the official votes after the polls shut on Election Day. Each voter would also be able, at their discretion, to verify the accuracy of the vote totals recorded by our blockchain voting system by auditing every ballot in the ballot box, all without disclosing the voter's identity.

B. Implementation

Forerunner the deployment of a blockchain-based decentralised online voting system. On the Ethereum blockchain, data is continuously stored. Because of the Ethereum blockchain, we can build code that can be distributed to a blockchain and have web nodes run it. In the application for this project. It is possible to develop decentralised applications and run them on the Ethereum virtual computer by utilising smart contracts in the Ethereum blockchain. This is the reasoning for the online voting system. Ethereum virtual machine smart contracts write the code and modify the reading and writing. A smart contract functions similarly to a microservice that is deployed via a network, transferring data in the form of value and executing any business logic that the programme specifies.. Node package manager, truffle frame (such as the MetaMask extension), work, and Ganache are required for the implementation of an online voting system. The package manager for Node.js is called NPM, and it is developed in JavaScript. Framework for truffles: Truffle is a blockchain development environment that uses the Ethereum Virtual Machine (EVM) to test frameworks and asset pipelines. Creating a system is not difficult for developers. Truffle controls the system's whole flow. To install truffle, do "npm install -g truffle" at the command prompt. by giving developers the opportunity to test and debug their applications with Ganache before putting them live on a blockchain network. In this application, a decentralised online voting system is developed using Ganache as local storage [13]. Google Chrome has an addon called MetaMask. MetaMask establishes a connection to the local Ethereum network for this application, enabling users to interact with previously developed smart contract applications through their personal accounts. The suggested application involves the following steps.

1) Open the folder on vs. code ide.
2) Install MetaMask on browser.
3) Install node js.
4) Download install ganache truffle.
5) Run app giving command on terminal.
6) Connect MetaMask and ganache
7) Give input as vote.
8) You will get an output
9) The system show expected result

IV. Experimental and Result Section

The system provides satisfactory results for voting using blockchain technology. To add the vote, the Voting UI calls a private function named addVoteFor (candidate name). The function generates a new block with the supplied data in it, along with a SHA256 hash of the user's data in the current block and the SHA256 hash of the previous block in the current block's data.After that, the completed block is verified and attached to the link.Since hashing is a one-way transaction, nobody will be able to undo it. The vote total will be visible to the public, but the user's identity will not be shared in any way. Vote counting can be done by calling a private method display totalVotesFor(candidate name) from the voting user interface. Because blockchain operates using a broadcast mechanism as opposed to traditional databases, the validity of votes cast is always ensured. It is OK as long as a particular block remains valid. As compare to existing system blockchain based solution is safe and takes less time . The performance of this system is improved.

Fig 4: Snapshot of Application

Fig 5: Snapshot of Candidate Selection

Fig 6: Snapshot for Election Voting Result

V. CONCLUSION AND FUTURE WORK

To overcome all the shortcomings of the current voting system, we want to use modern blockchain technology, an electronic voti ng system using blockchain. Using today's technology, the following goals can be achieved: -

Cheap voting, legal voting, fast voting. All citizens want to have a clearly visible certificate and direct democracy through electr onic voting using blockchain. People's confidence in voting is increasing and hence more people are coming out to vote, thus inc reasing the percentage of voters. The accuracy of voting was ensured by eliminating paper and pencil voting. Everyone loves tim e, and since the cost is reasonable, this electronic voting using blockchain is necessary for a transparent democracy. Ethereum's p rivate blockchain allows hundreds of transactions per second. Using smart contracts reduces the load on the blockchain. In count ries with large populations, blockchain should be used to add some additional technologies to electronic voting to prevent errors. The main reason behind this system is the emergence of the idea of using blockchain in voting.

REFERENCES

[1] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6. (2017)

[2] R. Krimmer, A. Ehringfeld, and M. Traxl, “The Use of E-Voting in the Austrian Federa-tionofStudents Elections2009,”(2018)

[3] Geneva Internet Voting System, www.coe.int/t/dgap/goodgovernance/Activities/Evoting/ EVoting_Documentation/ passport_evoting2010.pdf (2018)

[4] Raykar, N., Khedkar, G., Kaur, M. et al. A novel traffic load balancing approach for scheduling of optical transparent antennas (OTAs) on mobile terminals. Opt Quant Electron 55, 962 (2023). https://doi.org/10.1007/s11082-023-05201-0

[5] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing(CLOUD),SanFrancisco, CA, pp. 983-986 (2018).

[6] S.Ølnes, J.Ubacht and M.Janssen,"Blockchain in government: Benefits and implications ofdistributed ledger technology for information sharing", Government Information Quarter-ly. Barnes, C. Brake, T. Perry, “Digital Voting with the use of Blockchain Technolo-gy,”vol.34,, pp.355-364(2017)

[7] Raykar, N., Kumbharkar, P., Jayantilal, D.H. (2023). Assembled LSTM Technique Used for Phonetic-Based Algorithm for Demographical Data. In: Singh, S.N., Mahanta, S., Singh, Y.J. (eds) Proceedings of the NIELIT's International Conference on Communication, Electronics and Digital Technology. NICE-DT . Lecture Notes in Networks and Systems, vol 676. Springer, Singapore. https://doi.org/10.1007/978-981-99-1699-3_36 2023

[8] M. Pawlak,A. Poniszewska-Marańda and N. Kryvinska,"Towards the intelligent agentsforblockchaine-votingsystem,"ProcediaComputerScience, vol.141,pp.239-246,(2018).

[9] P. Tarasov and H. Tewari, "The Future of E-voting," IADIS International J. on Com-puterScienceandInformation Systems, vol.12,no.2,pp.148-165.

[10] Nagesh Raykar, Prashant Kumbharkar, Dand Hiren Jayatilal. Hybrid LSTM technique for phonetic. Int J Adv Electr Eng ;4(1):18-22. DOI: 10.22271/27084574.2023.v4.i1a.3 2023

[11] Bartolucci,S.,Bernat,P.&Joseph,D.SHARVOT:SecretSHARe-BasedVOTingontheBlockchain IEEE/ACM 1st International Workshop on Emerging Trends in Software En-gineeringfor Blockchain(WETSEB),30-34.(2018)

[12] Reyna, C.Martín, J.Chen,E. Soler and M. Díaz,"On blockchain and its integration withIoT.Challenges and opportunities",Future Generation Computer Systems, vol.88,pp.173-190(2018).

[13] Nagesh Raykar, Dr. Prashant Kumbharkar, Dr. Dand Hiren Jayatilal. De-duplication avoidance in regional names using an approach based on pronunciation. Int J Adv Electr Eng ;4(1):10-17. DOI: 10.22271/27084574.2023.v4.i1a.32 (2023)

[14] Wang, J.Sun, Y.He,D.Pang and N.Lu,"Large-scale Election Based On Blockchain", Proce-diaComputer Science, vol. 129, pp. 234-237(2018).

[15] https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake(2018)

[16] https://www.turkiye.gov.tr/(2018)

[17] Raykar,N., Kumbharkar,P.,Jayantilal,D.H.(2023).Structured Demographic Data De-duplication in Indian Names. In: Kumar, A., Ghinea, G., Merugu, S. (eds) Proceedings of the 2nd International Conference on Cognitive and Intelligent Computing. ICCIC 2022. Cognitive Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-99-2746-3_50

[18] Alharby, Maher, and Aad van Moorsel. “Blockchain Based Smart Contracts : A Systemat-ic Mapping Study. ”Computer Science & Information Technology (CS &IT) ,(2017)