

BALLOT CHAIN FOR SECURE AND TRANSPARENT ELECTION SYSTEM

1. ABIRAMI S
UG STUDENT CSE DEPT
NSN COLLEGE OF ENGINEERING AND
TECHNOLOGY –KARUR

2. INDHUMATHI S
UG STUDENT CSE DEPT
NSN COLLEGE OF ENGINEERING AND
TECHNOLOGY –KARUR

3. JANANI R
UG STUDENT CSE DEPT
NSN COLLEGE OF ENGINEERING AND
TECHNOLOGY -KARUR

4. ROSY R
UG STUDENT CSE DEPT
NSN COLLEGE OF ENGINEERING AND
TECHNOLOGY -KARUR

5. Mr. M. KARTHIKEYAN
ASSISTANT PROFESSOR CSE DEPT
NSN COLLEGE OF ENGINEERING AND
TECHNOLOGY -KARUR

I. ABSTRACT

Artificial intelligence (AI) has demonstrated huge potential in a variety of real-world applications. However, some significant considerations like fairness, transparency and trustworthiness are still challenging when applying AI to trust-oriented applications such as E-voting. The technology can ensure the safety of every vote, better and faster and much more accurate counting and automatic tallying. This method was aimed to facilitate the consolidation of AI ecosystems by developing a block chain-based traceable self-tallying e-voting system. The proposed system presents a novel voting system by using QR and Fingerprint of Aadhaar card. When the e-voting system is integrated with the Internet of Things, any eligible voter can vote from anywhere as there will be two or more levels of authenticity checks. The system permits the elector to cast their vote, block chain technology comes into

existence that is integrated within the machine. The proposed mechanism of voting using Block chain not only serves the election conducting bodies but also the voters who get notified in case of any meddling with their votes before the counting announcement.

II. PROBLEM IDENTIFICATION

India's current voting system is still fairly traditional and follows the age-old processes. Electoral frauds such as false voter registration, voter intimidation, and irregularities in tallying procedures are clandestine and illegal efforts to shape election result. Due to their illicit nature, it's hard to study the effects of these practices as political agents are careful not to leave trails. One of the reasons behind controversies associated with the choice of voting technology is that there is little systematic empirical evidence on the relationship between voting technology and election outcomes.

Electoral fraud undermines public trust in democratic conducting bodies. The potential contribution of the institutions creating political instability, and may affect long proposed framework is detailed as follows:

term growth. In India, many voters do not cast their votes. The security of IOT devices is ensured by analysing voting percentage generally is almost 50 to 60 percent their communication behaviours through social. Therefore, the representative bodies are not trust optimizer by ensuring their trust values. The representative. One of the main issues India is facing at present proposed mechanism is a two-end system, i.e., both is the declining voter turnout. The government attributes this the National election bodies and every entity may the fact that people have to vote from the constituencies where ensure the security upon compromise of IOT they have registered. Throughout the country, an estimated 450 devices through block chain mechanism. The million people have migrated from their hometowns for work proposed mechanism of voting using Block chain education, and so on, and many of them do not register in that not only serves the election conducting bodies but new constituencies.

also the voters who get notified in case of any meddling with their votes before the scheduled counting day.

Voters need to assemble at a centre allotted by the local authority to cast their votes. The process followed to collect and then count the votes has many irregularities that allow cheating and errors. Apart from the actual process, the counting of votes is a time-consuming activity. If any of the parties challenge the results, the recounting of votes, becomes cumbersome and consumes significant resource.

III. SCOPE OF THE PROJECT

This project has introduced a secure and transparent e-voting mechanism through trusted IOT devices using Block chain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. The trust of IOT devices is computed through a social optimizer that identifies their trust values by analyzing their communication behaviors. Further, Block chain technology plays a crucial role in coordinating the activities of legitimate IOT devices in the proposed solution. In order to prevent a prospective change of stored record of votes in databases, Block chain is maintained at various levels that keep track of all the recorded information handled by the election

IV. INTRODUCTION

This module uses the QR code and fingerprint biometric authentication provided by the Aadhaar card in India. Aadhaar card contains a citizen information, Aadhaar number, QR code. In that, Aadhaar QR code contains a valid Aadhaar number. By decoding the QR code, the Aadhaar number is obtained. The citizen information can be accessed by using the Aadhaar number. The citizen information contains an iris data, fingerprint data, address, etc. Based on the Aadhaar QR code, a virtual voting System using diary technique is developed. The AVS allows the citizen Aadhaar QR code. The Aadhaar number is extracted by the decoding of QR code. Extract the citizen information and fingerprint from the database based on the Aadhaar number. The individual's biometric features are captured and compared to previously captured and confirmed biometric features of that individual. All biometric data is first captured by a

sensor as an image. This image is then further processed into a biometric template. DCNN Algorithm used for verification and de-duplication are based on comparing these biometric templates.

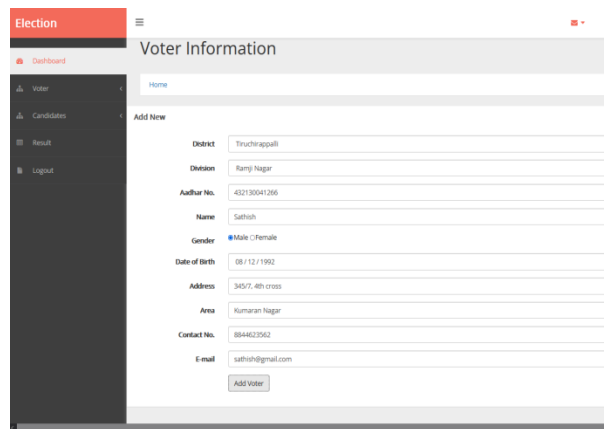


Fig1: VOTER VERIFICATION MODULE

Defining a smart contract includes identifying the roles that are involved in the agreement and the different components and transactions in the agreement process. The block chain application layer includes smart contracts, chain code and Ballot Chain. This layer comprises two sub-layers: 1) presentation layer and 2) execution layer. The presentation layer includes scripts, APIs, and user interface. These tools are used to connect the application layer with the block chain network. The execution layer includes smart contracts, chain code and underlying rules. The presentation layer sends instructions to the execution layer, which runs transactions. For example, instructions are sent to chain code in HF and smart contract in EV. The person is going to be allowed to vote for his or her desired candidate. During this step, once an individual completed his vote, a block is instantiated

and in real time hash code is calculated for the corresponding block, hash of the current vote in addition because the hash of the previous block is going to be hold on. This fashion every input is going to be unique and make sure that the encrypted outputs are going to be unique in addition. Block header records all the encrypted data of every vote solid. SHA-256 encrypts all the knowledge associated with each vote, and it's inconceivable to search out the encrypted hash function. If one block gets changed or tampered, the additional blocks from the tampered block will be modified. Hence change of state is not possible in the block chain.

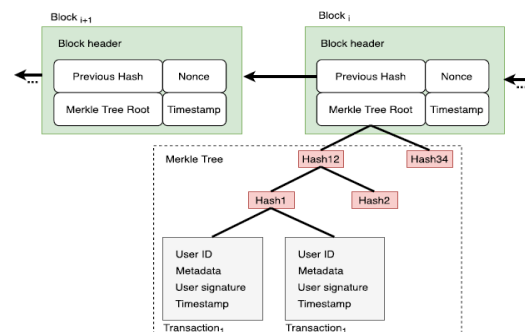


Fig2: Structure of the block

Each vote is added into each block encrypted by 256-bit SHA hash code, the hashed block cannot be tampered by any individual as more security is added to the system. Information within the block chain is placed up in an organized manner and hold on it blocs.

Each block has:

1. Information created
2. A time stamp of the block
3. An allude to the block

The third purpose, each block contains allude to the preceding block, that is that the main feature of Block chain. This reference helps to attach and build relations between each block.

Block chain is the solution to solve the issues that occur within the choice system.

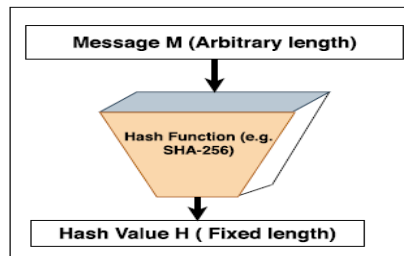


Fig3: HASH

To generate a digital signature of a message, the sender's signing algorithm produces a one-way hash of the message. A cryptographic hash function is a mathematical algorithm that takes an arbitrary amount of data input to map the content to a bit array of a fixed size called hash value or just a "hash". The hash algorithm is a one-way function which is practically infeasible to invert. The hash also known as the digest of the message is encrypted with the sender's private key. The digest along with other information such as the hashing algorithm is appended with the original message as a DS of the transmitted data. The receiver's signature algorithm verifies the electronic signature associated with the original content in two steps: 1) generating the hash or digest of the message, 2) decrypting the appended digital signature using the sender's public key. If both digests are identical, the data has not been changed. The tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. The final tally, the sum of all votes, which occurs when the deadline is reached, can then be obtained and verified, by any observer, against the product of all submitted ballots. In this module Artificial Intelligence applied to the

electoral count using Counting Sort Decision Algorithm. It is the most vital and robust module that has been developed to run on the Election Day for counting of votes, monitoring of end-to-end process and declaration of Results by the System. The Application is designed in a way that the series of work to be done by the Returning Officer in the System will automatically be popped up one after another. The counting result is announced by the ECI Authority after ending the election. When an election is over, the final result for each smart contract is published.

V. EXISTING SYSTEM

Current voting system is the conventional voting system built on ballot machine where the voter are allowed to cast their vote by pressing the button along with the symbol on the voting machine. E-voting system have been introduced using biometric technology which use face detection and recognition to cast their vote on their place without moving to polling booth. It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture

VI. PROPOSED SYSTEM.

In the proposed solution, all the activities are managed using a Block chain based mechanism. A two-end mechanism was proposed in which all the activities are coordinated by the national and state bodies at various levels and voters play an

equal part in it. The integration of Block chain mechanism and voting system may reduce the risks with transparent and decentralized feature of Block chain technology. The proposed method uses the QR code and fingerprint biometric authentication provided by the Aadhaar card in India. Aadhaar card contains a citizen information, Aadhaar number, QR code. In that, Aadhaar QR code contains a valid Aadhaar number. By decoding the QR code, the Aadhaar number is obtained. The citizen information can be accessed by using the Aadhaar number. The citizen information contains an iris data, fingerprint data, address, etc. Based on the Aadhaar QR code, a virtual voting System using diary technique is developed. The AVS allows the citizen Aadhaar QR code. The Aadhaar number is extracted by the decoding of QR code.

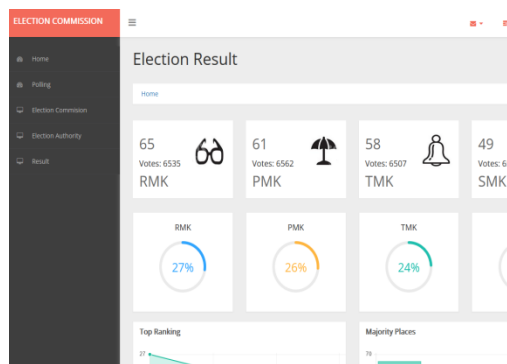


Fig4: ELECTION RESULT

VII. CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the

elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this project, we introduced a unique, block chain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the block chain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today's scheme and offer new possibilities of transparency.

Using a Ballot chain private block chain, it is possible to send hundreds of transactions per second onto the block chain, utilizing every aspect of the smart contract to ease the load on the block chain. For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second, for example the parent & child architecture which reduces the number of transactions stored on the block chain at a 1:100 ratio without compromising the networks security. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voter's vote is counted from the correct district, which could potentially increase voter turnout.

VIII. FUTURE ENHANCEMENT

In the future, it is aimed to simulate with a more realistic system, to operate the system from end to end, and to focus on optimizations for

scalability of the system. Another future work is that in the proposed system the end of election is assumed to be depending on the system time. However, the system may be improved to increase the security of the time dimension. In our opinion, transition to the e-voting method should proceed slowly by implementing in small pilot populations first and then widening the scope slowly. The implementation of such voting systems still possesses many challenges and risks for developers and governments.

IX. REFERENCES

- [1] S. Shukla, A. N. *asmiya, D. O. Shashank, and H. R. Mamatha, "Online voting application using ethereum blockchain," in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 873–880, Bangalore, India, September 2018.
- [2] S. Komatineni and G. Lingala, "Secured E-voting system using two-factor biometric authentication," in Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248, Iccmc, Erode, India, March 2020.
- [3] M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, and N. Sathisha, "Multimode authentication based electronic voting kiosk using raspberry pi," in Proceedings of the International Conference on I-SMAC (IOT in Social, Mobile, Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India., September 2018.
- [4] K. Curran, "E-voting on the block chain," =e Journal of British Block chain Association, vol. 1, no. 22–7, 2018.
- [5] M. Audi Ghaffari, An E-Voting System Based on Block chain and Ring Signature, School of Computer Science University of Birmingham, Birmingham, UK, 2017.
- [6] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, "Risks and opportunities of block chain based on e-voting systems," in Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 365–368, Chengdu, China, December 2019.
- [7] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Crypto currencies in blockchain technology: State-of-art, challenges and future prospects," Journal of Network and Computer Applications, vol. 163, Article ID 102635, 2020.
- [8] S. Bai, G. Yang, J. Shi, G. Liu, and Z. Min, "Privacy-Preserving oriented floating-point number fully homomorphic encryption scheme," Security and Communication Networks, vol. 2018, Article ID 2363928, 14 pages, 2018.
- [9] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," IEEE Commun. Mag., vol. 55, no. 9, pp. 16–24, Sep. 2017.

[10] M. E. M.Cayamcela and W. Lim, "Artificial intelligence in 5G technology: A survey," in Proc. Int. Conf. Inf. Commun. Technol. Conver. (ICTC), Oct. 2018, pp. 860-865.