IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN BASED E-VOTING SYSTEM

[1]Mr. Shreeyash Pednekar, [2]Mr. Bhushan Halasagi, [3]Ms. Chinmayee Kulkarni, [4]Mr. Adarsh Mulik, [5]Prof.Vaishali Latke

Department of Computer Engineering
Pimpri Chinchwad College of Engineering & Research, Ravet Pune, SPPU

Abstract: A blockchain is a distributed database that is shared by nodes in a computer network. Creating an electronic voting system that meets legislators' legal requirements has been a struggle for a long time. Distributed ledger technology is an intriguing technological innovation in the field of information technology. Blockchain technology may be applied to an almost infinite number of sharing economy-related applications. The purpose of this study is to look at how blockchain as a service could be utilized to build distributed electronic voting systems. The criteria for establishing electronic voting systems are elicited in this study, which also examines the legal and technological restrictions of implementing such systems using blockchain as a service. We provide a one-of-a-kind electronic voting mechanism based on blockchain that addresses all of the weaknesses we discovered. This study examines the potential of distributed ledger technology by detailing a case study, specifically the election process and the installation of a blockchain-based application that improves security and reduces the cost of hosting a national election.

Index Terms **- Cryptography, Blockchain, Distributed-Ledger, Smart Contract, E-voting, Aadhaar**

I. INTRODUCTION

Voting in India has long been a cause of heated dispute, whether it was the original "Balloting System" employed in the 1951-52 General Elections or the more recent "Electronic Voting Machines" widely implemented since 1998.In the balloting system, voters cast their ballots on pre-printed ballot papers in the presence of a voting official, and the total votes are gathered in a physical box and transported to a centralised vote counting station. The drawbacks with this approach were solved by switching to an electronic voting system, in which votes are captured on an electronic balloting device and transported to a central location, where they are calculated using a control unit. Electronic voting machines (EVMs) are claimed to be impenetrable to tampering. However, the system's reliance on an authority to monitor the voting process, as well as accusations of political party influence to support their cause, were two obvious problems.

Other difficulties with India's existing voting system include, but are not limited to, lack of transparency, fraudulent voter IDs, vulnerability to political manipulation in rural places, and delay in the announcement of results. All these difficulties can be effectively addressed by replacing any present voting choice with a blockchain-based electronic-voting system that functions on a user level and captures votes through a distributed interface (web/mobile). Wherever there is a requirement for transparency or decentralised authentication/identification of entities, whether currency, intellectual property, or else, blockchain technologies are frequently implemented. This encrypted, decentralised, and agile data storage system, guided by a government blockchain record, will result in a more responsive and user-friendly administrative collaboration. The goal of this article is to demonstrate the efficacy of a blockchain-based digital voting system that is more secure and transparent, and that is integrated with the UIDAI's Aadhaar identifying system.

II.PROBLEM STATEMENT

Building Electronic Voting System for an efficient, smooth and most secure way of voting using the Blockchain Technology.

III. LITERATURE REVIEW

"Decentralized Voting Platform Based on Ethereum Blockchain" by : David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb, present a novel strategy for a decentralised trust less voting network based on Block-chain technology to address trust issues. The system's major characteristics are data integrity and transparency, as well as one vote per cell phone number for each poll with guaranteed anonymity. The Ethereum Virtual Machine (EVM) is employed as the Blockchain runtime environment to do this.

Rifa Hanifa Tunnisa and Budi Rahardjo, "Blockchain Based E-Voting Recording System Design," states one solution to the challenges that frequently arise in the election system is blockchain technology. The use of hash values in recording the vote results of each polling station linked to each other makes this recording system more secure, as does the use of digital signatures.

The proposed sequence in the blockchain creation process in this system considers that in an electoral system where mining is not required, as in the Bitcoin system, because voter data and numbers are clear and voters are not allowed to select more than once, the proposed sequence ensures that all nodes which participate in the blockchain creation process are included.

Chaum, D, Essex, A, Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008)."Scantegrity: End-to-end voter-variable optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.Scantegrity is the first independent E2E verification mechanism that keeps optical scan as the underlying voting system and does not interfere with a human recount.

Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A fair and robust voting system by broadcast.", 5th International Conference on E-voting, 2012. This paper suggests a recovery round to allow for the announcement of the election result if voters abort, as well as a commitment round to assure fairness. Additionally, it gave a computational verification of ballot secrecy security.

Table 1. Literature Survey

Paper	Authors	Technique
Survey on Blockchain Based E-Voting Recording System Design	G Bhavani	AES Algorithm SHA 256 Algorithm
Decentralized Voting Platform Based on Ethereum Blockchain	David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb	1)HTML5 Webapp compiled with Apache Cordova 2)Ethereum network.
Online Voting: Voting System Using Blockchain	Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar	1)Cryptographic Verification 2)Homomorphic Encryption Technique

IV. BLOCKCHAIN

Blockchain is a system of storing data that makes it difficult or impossible to change, hack, or cheat it.A blockchain is a digital ledger of transactions that is duplicated and distributed across the whole network of computer systems that make up the blockchain. Each block in the chain comprises a number of transactions, and whenever a new transaction occurs on the blockchain, a record of that transaction is recorded to each participant's ledger. Distributed Ledger Technology (DLT) is a decentralised database managed by a number of people (DLT).Because it reduces risk, eliminates fraud, and enables scalable transparency for a variety of applications, blockchain is a particularly promising and revolutionary technology.

Benefits of Blockchain:

1. The ledger is dispersed across multiple locations: There is no single point of failure in the distributed ledger's upkeep.

2. Control over who can add new transactions to the ledger is spread.

3. Any proposed "new block" to the ledger must relate to the prior version of the ledger, forming an immutable chain that gives the blockchain its name and prohibiting tampering with previous entries' integrity.

4. Before a proposed new block of entries becomes a permanent part of the ledger, a majority of the network nodes must agree.

V. HOW DOES BLOCKCHAIN WORK?

Blockchain operates by hashing together blocks of data with a unique identity. This allows the current block to be linked to the previous block.

Hashing uses a mathematical procedure (SHA, AES, etc.) to transform an input string of fluctuating length into a cryptographic string of fixed length.

This hash is then used as an identifier in the next block of the blockchain, connecting it to the preceding one.

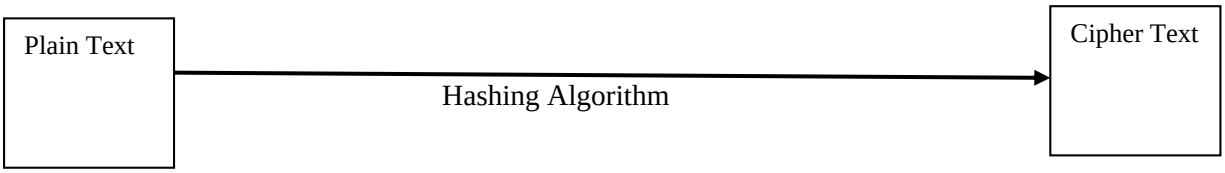

Figure 1. Hashing

Data that has been hashed cannot be decoded or traversed in the reverse direction (Fig. 1).

Furthermore, throughout any number of iterations, the hash for a specific input will always be the same.

VI. ARCHITECTURE

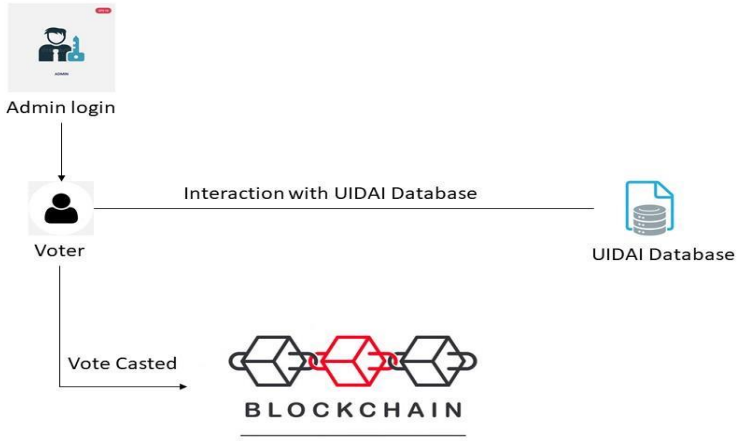

Figure 2. Architecture

In this model we are using the Aadhar number available to every citizen of India. The voting process will take place at a government-approved portal and the votes are recorded on a tamperproof instance that is open to the public for verification and validation. The Admin in charge will be responsible to login into the system and then allow voters to cast their votes.

After the admin logs in into the system the interface will ask the voter to enter his/her registered Aadhar card number .This Aadhar number will be validated with the Aadhar number present in the UIDAI database following a OTP verification process. After the OTP verification the voter can cast his/her vote and will be logged out .This will ensure that the voter can cast his/her vote only once.

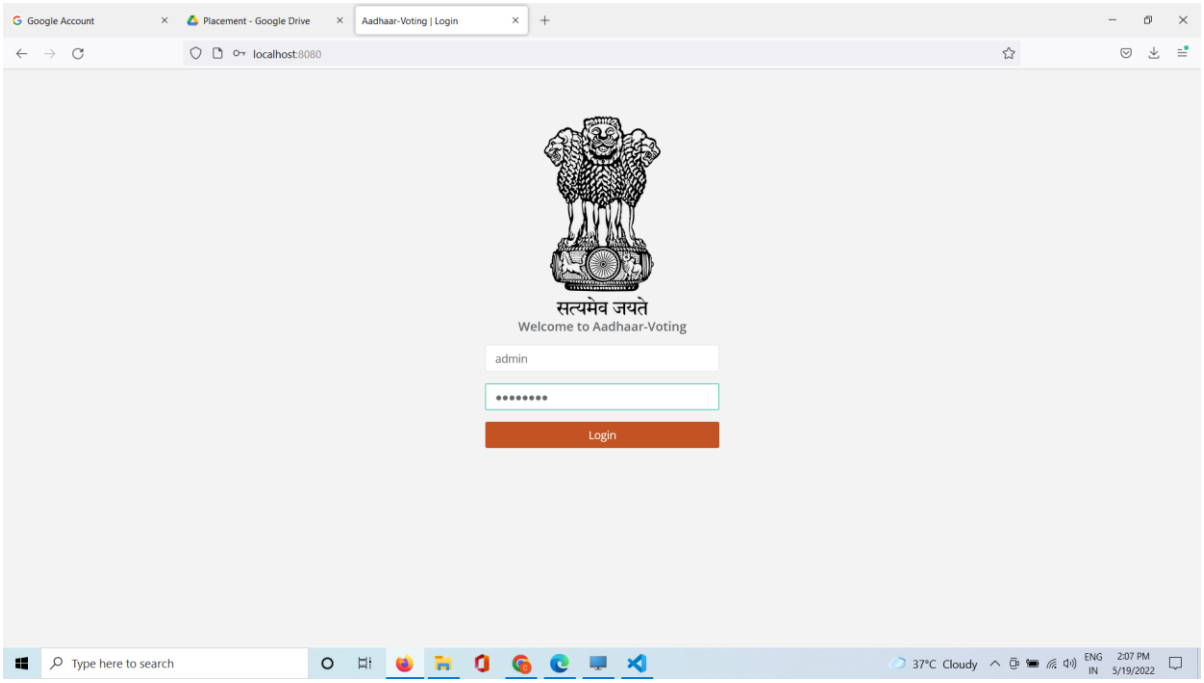

Figure 3. Admin Login Portal

VII. RESEARCH AND METHODOLOGY

The methodology is as follows:

1. Voting Interface

The voting UI will be created in such a way that the user may authenticate themselves using their unique Aadhaar ID. After completing the OTP verification request, the user can vote for the candidate of their choice.

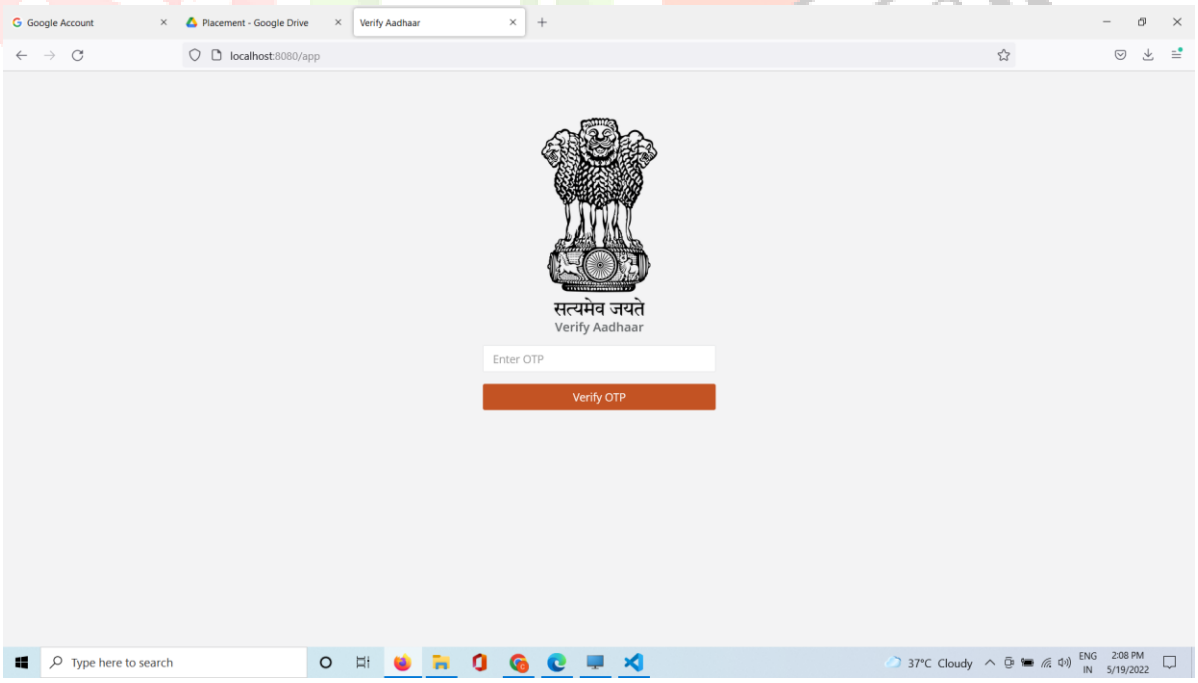

Figure 4. User Login using Aadhar

```
var aadhaar_no_phone_no = {
  "7382537xxxxx": "915801xxxx",
  "300000000000": "7720882192",
  "400000000000": "7758901612",
  "564357892578": "9767014966",
  "678900000000": "7887470268",
}
```

```
var aadhaar_list = {
    "300000000000" : "Akola",
    "738253790005" : "Bhandara",
    "564357892578" : "Pune",
    "678900000000" : "Mumbai"
}
```

Figure 5. Mock UIDAI Data Used

2. OTP Verification

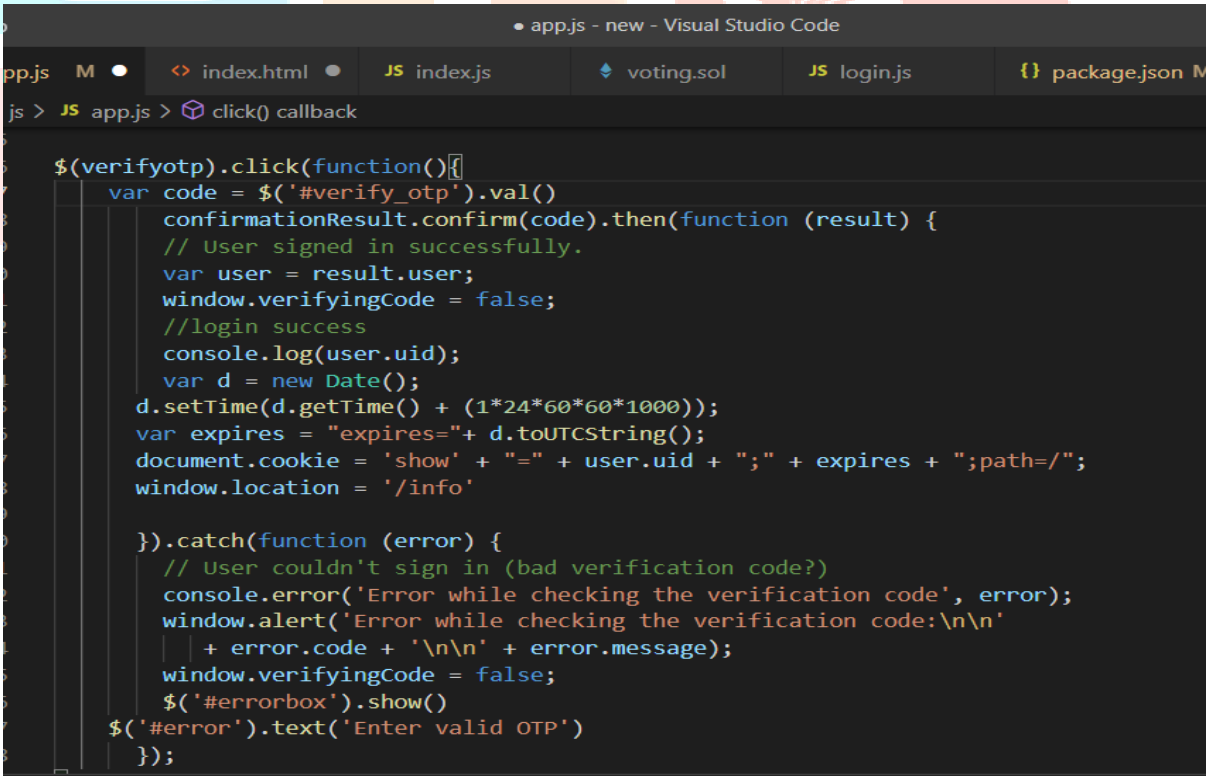

Figure 6. OTP Verification

3. E-Voting Blockchain

A private function addVoteFor(candidate name) is called from the Voting UI for the purpose of adding the vote. The function produces a new block containing the given data, as well as a SHA256 created hash of the user's data in the current block and the SHA256 generated hash of the previous block in the current block's header. Following that, the finished block is confirmed and put to the chain.No one will be able to reverse the hashing process because it is a one-way transaction. The user's identity will not be divulged in any way, even though the vote count will be available to the public. A private function display totalVotesFor(candidate name) can be invoked from the voting UI for vote counting.
The legitimacy of votes gathered is always guaranteed because blockchain works on a broadcast method rather than traditional databases. It is legitimate as long as a certain block is valid.

VIII. RESULTS AND DISCUSSION

After the submission of the vote to a particular party, the vote will be casted and stored inside a block which will not be then tampered at all and a dialogue box will appear showing the vote has been casted.

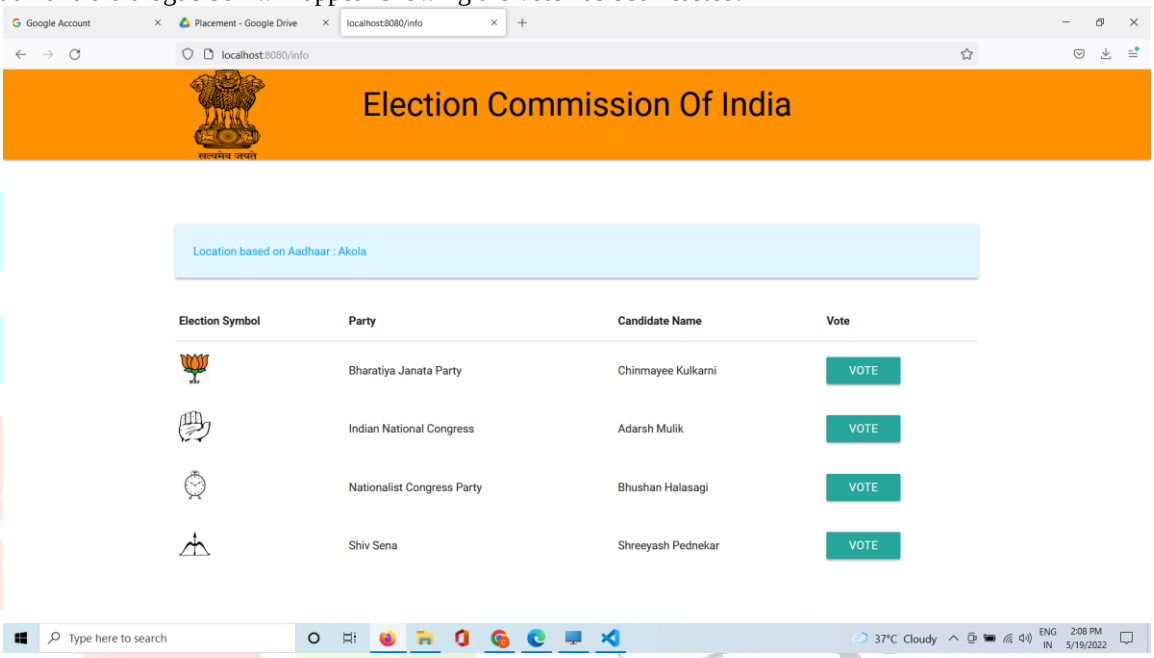

Figure 7. Candidates List

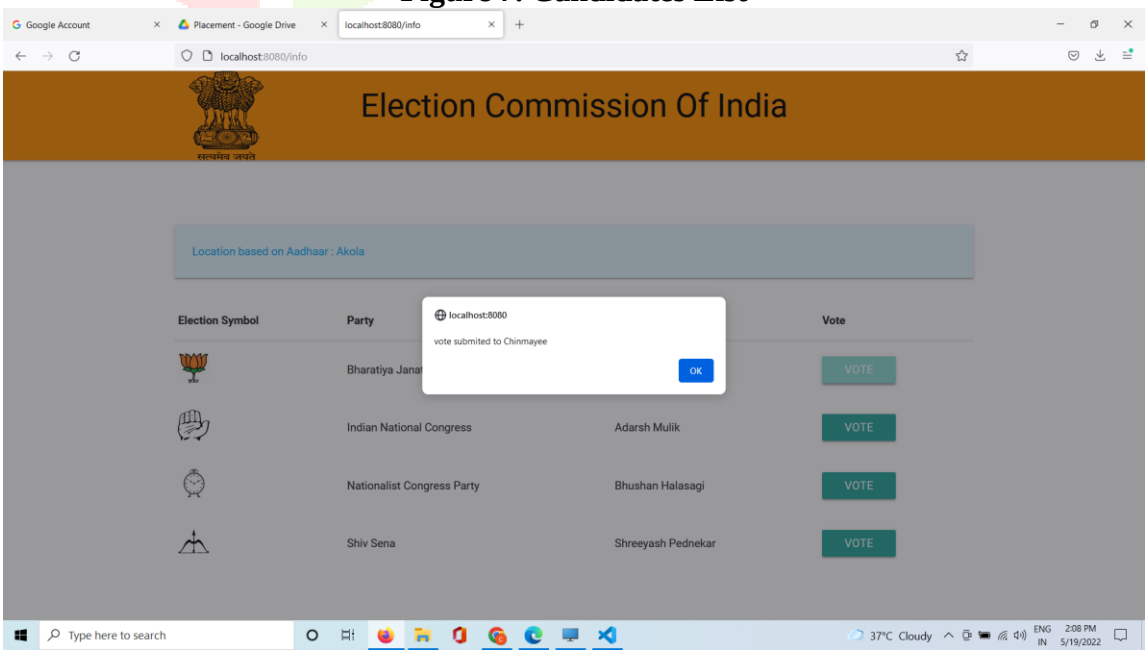

Figure 8. Vote Casted

IX. CONCLUSION

The blockchain's transparency provides for more auditing and knowledge of the elections. These characteristics represent a few of the requirements of a legal system. These qualities emerge from redistributed networks, and they have the potential to contribute more democratic processes to elections, particularly direct election systems. A viable solution for making e-voting more open, transparent, and auditable would be to use blockchain technology. Within the context of e-voting, this initiative demonstrates the potential and quality of blockchain technology. The blockchain will be publicly verified and distributed in such a way that no one will be able to tamper with it.
In today's society, the idea of adapting digital selection systems to make the general public electoral process cheaper, faster, and easier could be compelling. This style of electronic voting system assures the same while also delivering additional benefits such as instant electoral count, transparent and open-source voting platforms, and the ability for users to vote at their leisure.
According to reports, the Indian Election Commission spent INR 35000 crores on polling during the 2014 Lok Sabha elections. A significant portion of this sum is spent on the planning and setup of voting booths throughout the country. A digital implementation of the voting system can save a significant amount of money for taxpayers, which can then be used for other welfare programmes.

X. REFERENCES

[1] N. Satoshi, “Bitcoin: a peer-to-peer electronic cash system”, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 2018].

[2] J. L. Zhao, S. Fan and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue”, Financial Innovation, Springer Berlin Heidelberg, 2016, p. 2–28.

[3] D. Drescher, “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, 1 ed., Frankfurt am Main: Apress, 2017.

[4] G. Karame and E. Audroulaki, “Bitcoin and Blockchain Security”, Norwood, MA: Artech House, Inc, 2016.

[5] M. Risius, and K. Spohrer, “A Blockchain Research Framework - What We (don’t) Know, Where We Go from Here, and How We Will Get There”, Business & Information Systems Engineering, vol. 59, no 6, pp. 385–409, December 2017.

[6] C. De Faveri, A. Moreira and J. Arajo, “Towards security modeling of e-voting systems”, Proc. of IEEE 24th International Requirements Engineering Conference Workshops (REW), Beijing, China, 2016.

[7] F. Lehoucq, “Electoral Fraud: Causes, Types, and Consequences”, Annual Review of Political Science, vol. 6, no 1, pp. 233–256, June 2003.

[8] R. Qi, C. Feng, Z. Liu, N. Mrad and R. Qi, “Blockchain-Powered Internet of Things, E-Governance and E-Democracy”, E-Democracy for Smart Cities, Singapore, Springer, pp. 509–520, 2017.

[9] N. Mpekoa and D. van Greunen, “E-voting experiences: A case of Namibia and Estonia”, Proc. of IST-Africa Week Conference (IST-Africa), Windhoek, 201

[10] Roopak T M, Dr. R Sumatthi, “Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology”, Department of Computer Science and Engineering Siddaganga Institute of Technology 2019.

[11] Rifa Hanifatunnisa, et al, “ Blockchain Based EVoting Recording System Design”, School of Electrical Engineering and Informatics 2017.

[12] Vanessa Teague, Steve Schneider, Peter Y.A. Ryan, “End to End Verifiability in voting system from theory to practice” June2015

[13] R.Murali Prasad, et al, "AADHAR based Electronic Voting Machine using Arduino", International Journal of Computer Applications, vol. 145, no. 12, July 2016.

[14] Desna Sebastian, et al, "Aadhar Based ElectronicVoting System and Providing Authentication", International Journal of Science and Engineering Research (IJ0SER), no. 3, March 2015.

[15] Navya A et al, “Electronic voting machine based on Blockchain technology and Aadhar verification”. 2018 International Journal of Advance Research, Ideas and Innovations in Technology

[16] D Springall, T Finkenauer, Z Durumeric, J Kitcat, H Hursti, M MacAlpine, JA Halderman (2014), “Security Analysis of the Estonian Internet Voting System”, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.

[17] Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application", Available From http://www.id.ee/public/TBSPECEstEID-Chip-App-v3_5-20140327.pdf.

[18]UIDAI Aadhaar API, Available From https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf. 11 Bloomberg, "Why India's election is among the world's most expensive", The Economic Times, Accessed on Apr 7 2019.