

# SECURE VOTING SYSTEM USING BLOCKCHAIN

Dhanshree Aitwade, Rutuja Bhandare, Shraddha Dongare,  
Jyoti Chaudhary

aitwadedhanshri@gmail.com  
rutujabhandare7438@gmail.com  
shraddha.dongare99@gmail.com  
jyotikrjc@gmail.com



DEPARTMENT OF COMPUTER ENGINEERING  
JSPM'S IMPERIAL COLLEGE OF ENGINEERING AND RESEARCH  
WAGHOLI, PUNE 412207 SAVITRIBAI PHULE PUNE UNIVERSITY.

## ABSTRACT

Technology has positive impacts on various aspects of our social life. Designing a globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such innovation is blockchain – a keystone of crypto currencies. The blockchain technology is presented as a game-changer for many existing and emerging technologies. With its immutability property and decentralized architecture, it is taking center stage in many services as an equalization factor to the current parity between consumers and large corporations/governments. One future application of the blockchain is in e-voting. The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilizes the blockchain as a transparent ballot box. The protocol has been designed to achieve fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts.

**Keywords:** online voting, blockchain, crypto currency, Decentralized network, Cryptography, End to end verification.

## ARTICLE INFO

### Article History

Received: 30<sup>th</sup> April 2021

Received in revised form :  
30<sup>th</sup> April 2021

Accepted: 3<sup>rd</sup> May 2021

### Published online :

4<sup>th</sup> May 2021

## I. INTRODUCTION

Voting plays an important role in constructing a democratic society. The traditional voting requires voters to cast in appointed polling stations, which usually involves enormous expenditure on time and cost budget. E-voting, a new substantial online voting system which is structured on cryptography technique, has been gradually implemented and emphasised by people. The system supports full-function online voting by general household devices, and the entire polling results will be counted automatically and anonymously. Compared with traditional voting, electronic voting is a more economic system addresses on transparency and impartiality. As e-voting system mainly relies on the internet platform.

The crucial challenge for e-voting is the significant security risks it might cause. In order to reduce risks, in the past 40 years, various protocols related to the ballot-privacy,

individual verifiability, eligibility, completeness, fairness, uniqueness, robustness, universal verifiability and receipt-freeness have been widely proposed. Besides, the published protocols have implemented a variety of technologies, such as blind signature, ring signature, homomorphic encryption, Mix-Net, zero knowledge proof, etc In particular, the application of e-voting in digital currency has become gradually maturity nowadays. Based on the common security requirements of participants, this paper proposed a blockchain-based protocol associated with the priorities of the ballot-privacy, verifiability, eligibility, completeness, uniqueness, robustness, and coercion- resistance.

### Problem Statement:

To build a secure voting system, this will overcome challenges of current EVM, based voting system and offers fairness, transparency as well as flexibility.

## II. LITERATURE SURVEY

1. Title: Blockchain Based E-Voting System IEEE International Conference On Cloud Computing, Iceland, 2018 Author: Fridrik P. Hjalmarsen, Gunnlangur Description: Blockchain-based e- voting system that uses "Permissioned Blockchain". Cost efficient election while guaranteeing voter's privacy.

2. Title: Towards Secure E-Voting Using Ethereum Blockchain IEEE, Turkey, 2018 Author: Ali Kaan, Emre Yavuz Description: Integrating online election with Ethereum Blockchain Platform. Succeeded in moving e-voting to blockchain platform and addressed issues that legacy e-voting system by Using power of Ethereum network.

3. Title: A Proposal Of Blockchain- Based Electronic Voting System IEEE, Japan, 2018 Author: Cosmas Krisna Adiputra, Rikard Hjor Description: Combine the idea of double envelope encryption and blockchain technology. Used blockchain for electronic voting system.

4. Title: Blockchain-Enabled E-Voting IEEE, Korea, 2018e Author: Nir Kshetri, Jeffrey Voas Description: Used digital currency(coin) analogy for casting a vote. Addresses voter tampering, promote more voter participation, greater transparency and security.

5. Title: Blockchain Technology Innovations IEEE, USA, 20 Author: Tareq Ahram, Arman Sargolzaei Description: Application of blockchain in various fields. Identified blockchain as a catalyst for emerging use cases in financial and non-financial industries.

### III. PROPOSED SYSTEM

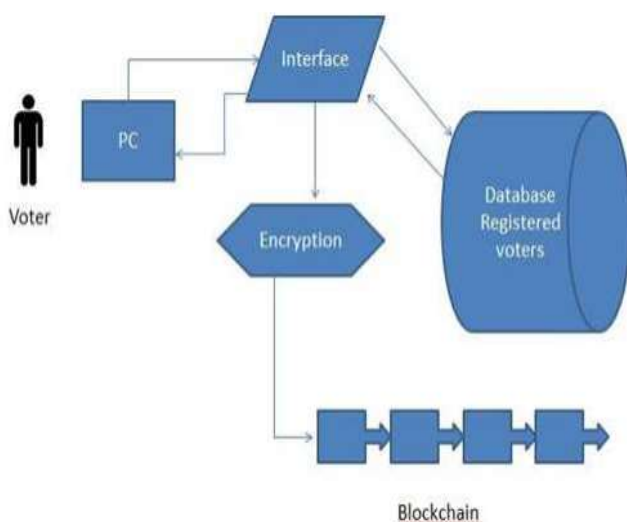


Fig 1. E Voting System Architecture

#### A. Description:

Proposed system is an internet voting system. We provide an online platform for voting i.e a website. Propose system three parts as Voter, Election Administrator and Election Process.

A) Voter : Voter is the main part of the system which participate in the election process. He register himself in system by giving his personal information.

B) Election Administrator : To manage all the data coming from voter during registration.

C) and election process, election administrator has worked. Also it generate public and private keys for voters. It is nothing but python packages.

D) Election Process : In this process voter select the candidate to vote and give his vote for selected candidate.

#### B. Mathematical Model

System Description: RSA algorithm is a kind of asymmetric cryptographic algorithm which is used to encrypt and decrypt the messages. Its security is based on the difficulty of large integer decomposition. There are many implementations in reality.

The specific algorithm can be described as follows.

1. Choose two different large prime numbers.
2. Define  $n = pq$ ,  $(n) = (p-1)(q-1)$ .
3. Choose  $e [0, (n) 1]$ .
4. Calculate the modular multiplicative inverse of  $(n)$  as  $d$  which ensures  $ed = 1 \text{ mod } (n)$ .
5. Define  $e, n$  as public key and  $p, q, d$  as private key Where, Decryption: Give the ciphertext  $y$ , compute  $x = y \text{ mod } n$  to encrypt the message by using the private key  $(p, q, d)$ .

Constraint: Constraint C = User should login to the system for voting

Function: Success Conditions: Successfully transaction of vote.

### IV. CONCLUSION

Blockchain Technology is gaining popularity day by day. Using blockchain in voting system will help to achieve secure and cost-efficient election while guaranteeing voter's privacy. Also, due to the encryption mechanism, it is impossible for any person to gain access to all the votes without first taking control of the entire service network.

### V. ACKNOWLEDGEMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am heartily thankful to my project guide for his valuable guidance and inspiration. In spite of their busy schedules they devoted their self and took keen and personal interest in giving us constant encouragement and timely suggestion. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

### REFERENCES

- [1] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, " A Proposal of Blockchain-based Electronic Voting System " Dept. of Electrical Engineering and Information

Systems. Artis Mednis, Girts Strazdins, Reinholds Zviedris, Georgijs Kanonirs, Leo Selavo, "Real Time Pothole Detection using Android Smartphones with Accelerometers."

[2] Fridrik P. Hj' almarsson, Gunnlaugur K. Hreidarsson, Mohammad Hamdaqa, G'isli Hj' almt' ysson, "Blockchain-Based E-Voting System ". Available at: <https://ieeexplore.ieee.org/document/8457919>.

[3] Ali Kaan Koc, Umut Can abuk, Emre Yavuz, Gokhan Dalkoloc, "Towards Secure E-Voting Using Ethereum Blockchain". Available at: [ieeexplore. ieee.org/document/8355340/](https://ieeexplore.ieee.org/document/8355340/).

[4] Henry Rossi Andrian, Novianto Budi Kurniawan, Suhardi, "Blockchain Technology and Implementation : A Systematic Literature Review". 2018 International Conference on Information Technology Systems and Innovation (ICITSI) October 22-25, 2018.

[5] Nir Kshetri and Jeffrey Voas, "Blockchain-Enable Voting", <https://Blockchain>.

[6] Basit Shahzad and Jon Crowcraft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology."

[7] Tareq Ahram, Aman Sargotzaei, Saman Sargotzaei, Jeff Daniels, Ben Amaba, "Blockchain technology Innovations". Available at: [https://ieeexplore. ieee.org/document/7998367/authors](https://ieeexplore.ieee.org/document/7998367/authors)

[8] Rishav Chatterjee, Rajdeep Chatterjee, "An Overview of the Emerging Technology: Blockchain". Available at: <https://ieeexplore.ieee.org/document/8307344>.

[9] Christopher G. Harris, "The Risks and Challenges of Implementing Ethereum Smart Contracts ". Available at: <https://ieeexplore.ieee.org/document/8751493>.

[10] H Halpin, M Piekarska, "Introduction to Security and Privacy on the Blockchain", 2017 IEEE European Symposium on 2017 - [ieeexplore.ieee.org](https://ieeexplore.ieee.org).