ISSN 2395-1621

IMPLEMENTATION OF ONLINE SECURE VOTING SYSTEM USING BLOCKCHAIN

Dhanshree Aitwade, Rutuja Bhandare, Shraddha Dongare,
Jyoti Chaudhary, Prof. Vaishali Bhorde

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: 5th June 2021

Received in revised form :

5th June 2021

Accepted: 7th June 2021

Published online :

8th June 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.Much like the early days of the internet, widespread adoption of this technology will take time but as highlighted from the excerpt of Blockchain Revolution below surprising steps

towards this goal are happening and effecting not just how we vote but how we create policy as a whole.

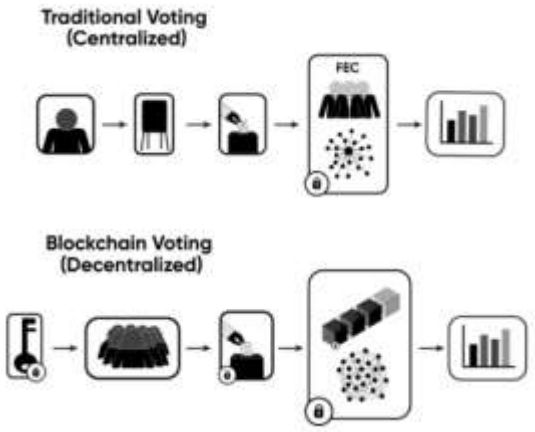

Fig 1. Difference between traditional and block chain concept

II. PROPOSED SYSTEM

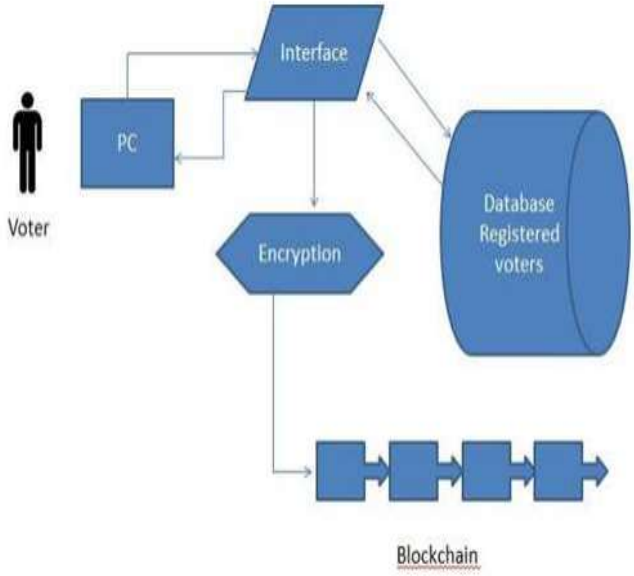

Fig 2. E Voting System Architecture

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 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 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.

III. ALGORITHM AND TECHNOLOGY USED

Algorithm:
1. SHA3- 256 Algorithm :
• Secure Hash Algorithm is one of best algorithm to generate hash value from data.

• SHA-256 is having fixed length hash value i.e 64 bit

• It is one way encoding algorithm so that it is impossible to generate original message from hash value.

• Miner change in input will change hash value drastically.

• It is helpful to handle the collisions, means two different data cannot have same hash value. So it is too much secure.

2. RSA (Rivet-Shamir-Adleman) Algorithm :
RSA is asymmetric cryptographic algorithm which is use to encrypt and decrypt the messages.

Technology:
• Python : Python language is used to build Blockchain.

• Django : Django is a Python-based free and open-source web framework, which follows the model-view-template architectural pattern. Django's primary goal is to ease the creation of complex, database-driven websites.

• Data Structure : Structure of Blockchain is like doubly linked list. Each block has hash of previous block, data and hash of current block.

• Database : MySQL is open source structured database which provides data security and high performance.

IV. RESULT

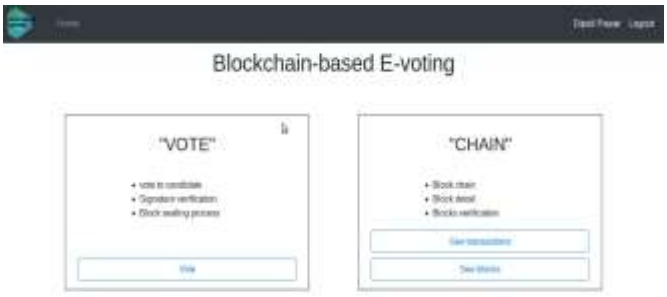

Fig 3. Home Page

Fig 4. Voting Page

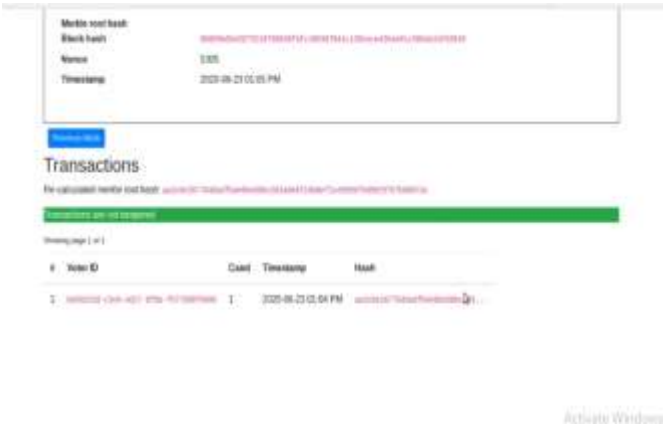

Fig 5. Secure Voting Process

V. 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.

VI. 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´ısli 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/.

[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

[8] Rishav Chatterjee,Rajdeep Chatterjee,"An Overview of the Emerging Technology:Blockchain". Availabl at:https://ieeexplore.ieee.org/document/ 8307344.4

[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.

