EmergIN
Innovation- Excellence- Sustainability
International Conference on Emerging Technologies and Innovations

01-02 March 2023

Voting System Through Blockchain Technology

Akshat Dubey[1] , Muskan Sharma[2], Abhishek Sharma [3], Vatika Jalali [4]

[1](Department of CSE(Internet of Things), Noida Institute of Engineering and technology, India)
[2](Department of CSE(Internet of Things), Noida Institute of Engineering and technology, India)
[3](Department of CSE(Internet of Things), Noida Institute of Engineering and technology, India)

Abstract

Electronic System or e-voting system has been used from the 70's with the benefit of security and efficiency. General election uses a centralisation system i.e one organization that manages it but the blockchain uses the decentralized method in this entire database is owned by many users. By using blockchain in the voting system, reduce the chances of cheating and manipulation of the data from the database.

At this stage, technological use is crucial for assisting in meeting human requirements. Given that most people nowadays don't trust their governments and that elections are crucial in contemporary democracies, the growing use of technology has brought new difficulties to democracy. Elections are crucial in deciding who will lead a country or organization, or you might say that they are the event that determines the future of any nation. The paper provides a thorough assessment of the system, effectively demonstrating its ability to produce an end-to-end verifiable e-voting system.

Keywords- Blockchain,ethereum,e-voting,smart-contract,solidity

1. Introduction

Elections are a crucial component of a democratic society because they give the general population the opportunity to voice their opinions by voting. Due to its importance, the election system should be transparent and reliable for society. It is equally important to political welfare.Secure multi-party computation is a type of secure electronic voting. A group of people cast their votes in a democratic method, and those votes must be kept secret. Blockchain provides a decentralized mechanism in the voting system. In blockchain there is no one person who has all the charges. Unlike traditional system blockchain come into existence with the concept of decentralization . Every node contains data and each node is connected with another node. If one node's data changes all the nodes need to be changed i.e millions of nodes are interconnected which is hard to change. It uses the pseudonymized network for the security level.

The system uses threshold encryption without a trusted third party to make sure that no one could tally the election results before it was over. Furthermore, even if the election administrator is acting maliciously, the final results will stand. A pair of public and secret keys are created as part of the encryption process. All parties have access to the secret key in parts; however, no party has access to the entire secret key prior to the key reconstruction stage. The secret key is rebuilt when at least n parties contribute their secrets.[1]

A smart contract is used to deploy the voting system on Ethereum. With the help of the Ethereum script, users can create the necessary smart contracts on Ethereum and leverage those contracts' strong features to build decentralized applications. To confirm the validity of the outcome, the contract code is separately run on each node of the Ethereum network. The outcome is openly verified. [2]

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

The rest of the paper contains the followup sections: the next section is the literature survey in which existing system working and technique used is defined. Section 2.2 presents the limitation of existing system or research gaps that define where they are lacking with technique. After this methodology is elaborated and then followed by the result and conclusion of the project.

2. Literature Review

2.1 Survey Existing system

1. *A. A. Lahane, J. Patel, T. Pathan, and P. Potdar, "Blockchain technology based e-voting system," ITM Web of Conferences, vol. 32, p. 03001, 2020.*

   This paper more focused on the loopholes in the current voting (offline) system and described that online voting system is better than offline voting system in terms of legality and security.It additionally describes how blockchain can be used for casting votes with security. Proposed solution in this paper uses no blockchain-based platform to deploy voting protocol rather than hashing is used for connecting blocks.[2]

2. *P. M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "Blockchain based e-voting system,"International Journal of Scientific Research in Science and Technology, pp. 134–140, 2021.*

   This paper proposed that the decentralized system is better than the centralized system as the database manipulation is very easy in a centralized system. This paper proposes the solution of deploying voting protocol on Ethereum blockchain and encryption i s done using a pair of public and private keys.Additionally it includes the gas cost , encryption method , technology used by different authors in their paper.[1]

2.2 Limitations of Existing system or Research gap

Current system does not have a verified authentication method to match digital identity of voters during casting of vote and is less focused on implementation of e-voting systems using blockchain. However, it is primarily focused on how online voting systems can be better than the traditional voting system. Another limitation is the cost of gas used in blockchain voting systems as it is expensive and can require large money to conduct big elections.

2.2.1 Problem Statement

To provide a proper system that authenticates voters and makes the voting process easy, reliable, and remotely accessible by using blockchain technology and making it efficient with more affordability.

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

3. Proposed Methodology

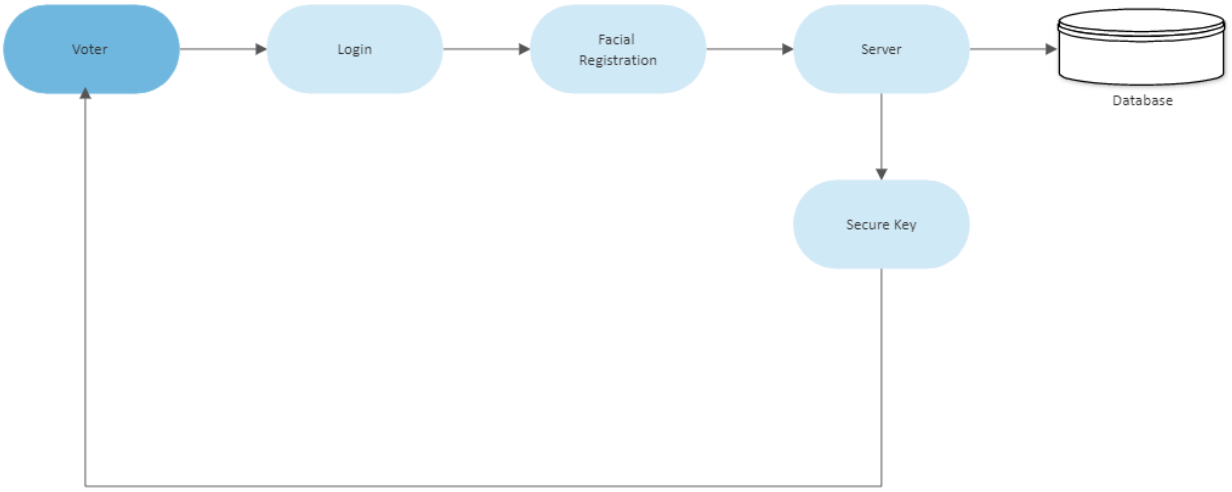


Figure 1. Pre-Voting Process

To cast the vote, users first have to login using mobile number and email id to the voting portal prior to the day of voting and should get registered with facial registration. A secret key will be generated by the server and will be provided to the voter. Voters will only be able to cast a vote after entering this secret key on voting day.

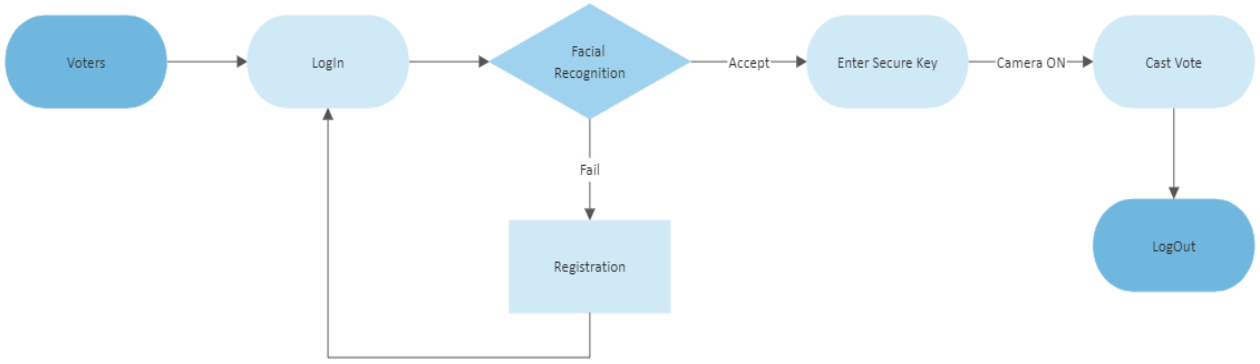


Figure 2. Voting Process

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

On the day of voting, voter will first have to login using mobile number and email id afterwards face of the voter will be recognised if it is matched one from database than voter will allow to enter the provided secret key for authentication and if it gets mismatched than voter must have to register himself first and repeat the process again, after recognition voter can cast their vote , during casting camera of the device will be on for the supervision of voters.

3.1 RSA algorithm to generate public and private keys [2]

1. *Select two large prime numbers, p and q.*
2. *Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.*
3. *Choose a number e less than n, such that n is relatively prime to (p - 1) x (q -1). It means that e and (p - 1) x (q - 1) have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd (e,d(n)) =1*
4. *If n = p x q, then the public key is <e, n>. A plaintext message m is encrypted using the public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.*

   $C = m^e \bmod n$

   Here, m must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
5. *To determine the private key, we use the following formula to calculate the d such that:* $D_e \bmod \{(p - 1) x (q - 1)\} = 1$

   Or

   $D_e \bmod \varphi (n) = 1$
6. *The private key is <d, n>. A ciphertext message c is decrypted using the private key <d, n>. To calculate plain text m from the ciphertext c the following formula is used to get plain text m.* $m = c^d \bmod n$

3.2 Implementation

Ethereum blockchain can be one of the good options for building blockchain based voting systems. It provides the ability to make smart contracts, the term "smart-contract" refers to the program or protocol that performs a particular activity when a particular condition is met.[4]

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

3.2.1 Truffle

Truffle is a development environment for building projects over ethereum blockchain, it has features like automatic contract testing , contract administration and network management for deploying to any number of public and private networks.

3.2.2 Solidity

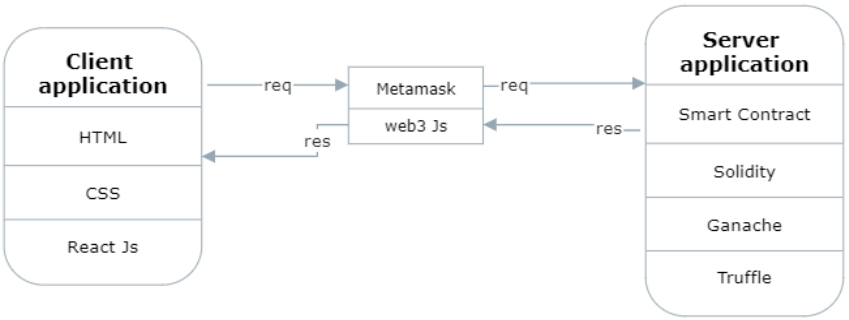
Solidity is the object oriented ,high level programming language for implementing smart contracts.It is also designed to operate ethereum virtual machines.

3.2.3 Ganache

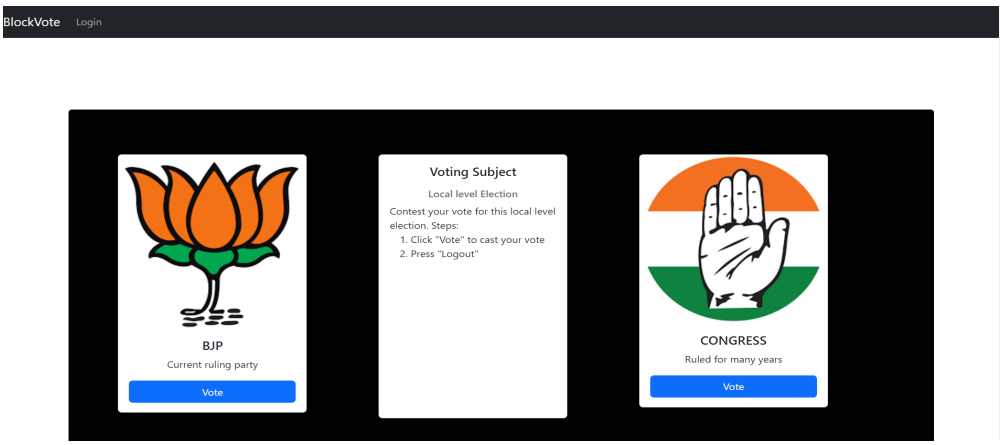
Ganache is the tool used for testing and managing blockchain applications on the local machine, it is a blockchain simulator installed locally to update, reuse and test the decentralized application.

3.2.4 Node Server

It is the server to which users interact and use for the generation of private-public keys with which it also encrypts casted votes.



4. Results



Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

5. Conclusion

In this paper we analyzed that using blockchain technology we can change the traditional voting process and make it more reliable , transparent , convenient and simple for voters. With the property of a decentralized network of blockchain we can make voting secure and accessible.This paper discussed the authentication process for users and implementation of blockchain in the voting process and technology required to make it possible.

The idea of adapting blockchain technology for voting makes the process low-cost and quick normalizes it in the eyes of the electorate, dissolves an explicit power barrier between them and the functionary, and applies a clear amount of pressure to the latter. Additionally, it makes way for a more direct kind of democracy where citizens can express their opinions on certain proposals and measures.

References

Journal Papers:

[1] P. M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "Blockchain based e-voting system," International Journal of Scientific Research in Science and Technology, pp. 134–140, 2021.

[2] A. A. Lahane, J. Patel, T. Pathan, and P. Potdar, "Blockchain technology based e-voting system," ITM Web of Conferences, vol. 32, p. 03001, 2020.

[3] K. M. Khan, J. Arshad, and M. M. Khan, "Secure Digital voting system based on Blockchain Technology," International Journal of Electronic Government Research, vol. 14, no. 1, pp. 53–62, 2018.

[4] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of Digital Voting System Voting System," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 6855–6871, 2022.

***Website*:**

[5] "RSA encryption algorithm - javatpoint," www.javatpoint.com. [Online]. Available: https://www.javatpoint.com/rsa-encryption-algorithm. [Accessed: 07-Feb-2023]

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.