A Transparent Immutable and More Secured Voting System Using Blockchain

S Nagajothi*, S S Shamrutha, D Sreeja, and S J Tejeswini
Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India
Email: *nagajothis@skcet.ac.in

Abstract. Blockchain is a cryptocurrency system with a transaction record of several computers in a peer-to-peer network. Blockchain In this paper, we propose a transparent, immutable, and more secured voting system using blockchain that collectively approaches security and cost issues. In Ballot voting, there is no security, immutability between the voter and the system. The proposed system uses blockchain technology to increase the efficiency of the voting system. Here the algorithm used is blockchain which includes a private key and public key encryption, SHA-256, Merkle hashing tree, and for security, one-time password (OTP) authentication can be done. It permits the voter to vote from any place, which increases the overall attendance percentage. The proposed system gives improved security and manages several data in the blockchain. In this system, we proposed security voting by using blockchain technology. In the existing system easy to vote for the ones who have not voted? I, vote fraudulent is happening on every century, some securities have been implemented but in parallel fraudulent is also increasing. People should reach the respective booth to cast their vote, which will affect their day-to-day life regularities. There is no transparency to the voter whether his/her vote is counted or not. The acknowledgment is not provided to the user after voting. Here we overcome these issues and provide more security, transparency, and immutability.

Keywords: Blockchain, Internet of things, Immutable, cryptographic hash value, voting system.

1. Introduction

The project's objective is to protect the people's vote using blockchain technology [15]. It allows the voter to cast their vote anywhere, i.e., the voting system in online through government websites [5]. Democracy is the system every citizen must know the election vote and rights [4]. In the existing system easy to vote for the ones who have not voted? I, vote fraudulent is happening on every century [7] people need to trust their voting system, some securities have been implemented but in parallel fraudulent is also increasing [8]. People should reach the respective booth to cast their vote, which will affect their day-to-day life regularities [9]. There is no authentication on the polling station, so it is easy to cast a vote for the one who has not voted. In some areas, the voting station is too far, so the voters prefer not to vote. There is no transparency to the voter whether his/her vote is counted or not [11]. The acknowledgment is not provided to the user after voting. Here we overcome these issues and provide more security, transparency, and immutability.

In today's system, all people have the right to vote given by the government. They need a secured voting system. The system that is being proposed makes the election process more secure, transparent, and immutable and can be used in current situations. The blockchain structure is an append-only data structure. Append-only is a property of computer data storage. Here existing data is immutable, where new data can be appended to the storage. Each block is independent in nature they depend on the previous block, assuring immutability. E-voting replaces the ballot voting system [13] to increase efficiency in the system. Several studies say that ballot voting has less security, and several frauds may
occur in voting. By using effective hashing techniques, this system will give the security of the data. To implement the system, we need to create a block and sealing the block. Using the polling process, the election authority has a blockchain; it creates and seals the block and announces the result. This is an effective method to implement a safe and secured voting system. By using blockchain, this system implements a safe voting system.

**Transparency:** The system is transparent to the user and admin, and there is assurance his/her vote is counted. The candidate name and party name are encrypted using a private key in blockchain technology. The transactions made in this system use a high-security system, so data theft is not possible in the blockchain system. In case of any changes need in data transactions, the whole block needs to be changed according to the same set of rules. So, changes are impossible.

**Security:** One-time password (OTP) authentication is used to provide more security. Once it is confirmed, voters can vote; otherwise, it is already voted or not enrolled. In the voting process, data exchange is achieved through Internet of things (IoT).

**Immutability:** This is the efficiency of the system that cannot modify. So changes cannot be implemented in the blockchain, i.e., it is not possible to alteration. Immutability is the essential feature of every single blockchain. Stability is the only condition for double-spending detection. Double spending cannot be possible in ledger content. So it is not possible to change the double-spending. This proposed work provides more security and flexibility using blockchain technology, which includes public and private key encryption, SHA-256, Merkle hashing tree.

2. **Existing System**
From the traditional period, vote fraudulent is happening every century; some securities have been implemented, but in parallel fraudulent is also increasing. People should reach the respective booth to cast their vote, which will affect their day-to-day life regularities. No acknowledgment was provided to the voter.

3. **Literature Review**
Several algorithms have been implemented for a voting system in the blockchain system. For exchanging data, the system uses IoT. It is a very efficient method for data exchange. This paper's disadvantage is that the user has no assurance that his/her vote is counted, and it requires a ballot voting machine to cast their vote, which is highly economical [1]. The research paper evaluates the description of the election process and improves the security of data. The cost of the system is very low. The disadvantage of this paper is that it requires a unique id and PIN to cast their vote. [2]. several studies give details on the process of polling [3]. By using a blockchain system, the whole algorithms for the voting process are implemented. This system's disadvantage is that the Private Key is not generated to get their acknowledgment, and voters need to visit their respective booths to cast their vote[4].

Several countries implement the Internet-based voting system. By using some official websites, it will support voting for every person. Several measures implement the e-vote system [6]. The election must have happened in a secured system, and it ought to increase the efficiency of the voting system [10]. This paper will give the security on voting. Several countries have a security analysis on their voting system. In India, several studies show the security protocol on the voting system [12]. Through mobile, we can vote our vote, but it is not an efficient method for the user who cast their vote [14].

4. **Proposed System and Architecture**
This proposed work provides more security and flexibility using blockchain technology, which includes public and private key encryption, SHA-256, Merkle hashing tree. This ensures that users can cast their vote exactly once; we use the one-time password (OTP) for authentication. The voting is transparent to the user as a private key is sent to the user to track and view the vote status. The voting
can be done anywhere, so the attendance percentage is increased, and even the election results can be declared as soon as the voting process is over. The vote of the user is secured, immutable and transparent. The proposed system architecture is shown in Figure 1.

The acknowledgment is provided to the user after voting by sending a message to the registered mobile number. The data flow is shown in Figure 2. Here the data flow is implemented in those steps. Figure 3 shows the use case chart for the voting person for his verification. Figure 4 shows the system's sequence; this will give the communication between the voter and the admin with the system.

![Proposed Architecture](image1)

**Figure 1: Proposed Architecture**

![Dataflow chart](image2)

**Figure 2: Dataflow chart**
A. Candidate and User Registration
This is the first module of our project; in candidate and user registration, the candidate information, aadhaar number, and the area he is standing are filled by the admin and his mobile number. The user also gives his all the necessary detail along with his mobile number. The user enters into his login page using his aadhaar number, and authentication is done to cast his vote. Figure 5 shows the registration for the user and the candidate.

B. Server Deployment
In our second module, the user and candidate details are collected, copied, and stored in the database using the local server, as shown in Figure 10.

C. Authentication
In authentication, we have used one-time password (OTP) authentication to verify the user and candidate. Once the authentication is verified and confirmed, he/she can cast their vote or else they are blocked to proceed, which means they have already voted or not enrolled for the election. Figure 6 shows the authentication system.

D. Vote Casting
In vote casting, after authentication on the voter, they are allowed to cast their vote for the area using the registered aadhaar number. It allows the voter to cast their vote anywhere. It is shown in Figure 7.

5. Blockchain Formation

A. Creation of Block
By using SHA 256 algorithm, this system implements the hash value to create the block. The created hash value with the other information is stored in the header. Using a new hash value, we can build the next block and link with the existing hash value.

Block1 = hash (Uid +hash value 1)
Block2 = hash (Uid +hash value1 +hash value 2)

B. Block Sealing
If a person votes and all transactions they used are recording in the blocks, the blocks are to be sealed with the hash and Merkle hash tree after the voting process. So after the polling time, the seal for the block is essential. Figure 8 shows the blockchain formation.

Sealed Block1 =hash (hash (pairs of transactions) +hash of block 1)
Sealed Block2=hash (hash (pair of a transaction) +hash of block1+hash of block 2)
6. Implementation
Acknowledgment is sent to the voter that they have successfully voted along with their block number in which it is stored. Merkle tree records the distribution of the block. If the voters vote registered successfully, it will create a message to the voter as your vote has been successfully cast and stored in block number of: 0 as shown in Figure 11. The result is collected through the data stored in the blocks with the nodes in the blockchain. If the polling time is ended, the result can be declared immediately, as shown in Figure 12. So the result is declared with the help of data stored in the system. Figure 9 shows the registration page.

Figure 8: blockchain formation

Figure 9: Registration

Figure 10: Server deployment
7. Conclusion
Thus, blockchain's power has been used adjustably to fit into the dynamics of the electronic voting process. It guarantees that each vote is counted in a correct manner, which could potentially increase the voter's attendance, and acknowledgment is sent to the voter along with their block number in which it is stored. Acknowledgment is sent to the voter that they have successfully voted along with their block number in which it is stored. The acknowledgment is provided to the user after voting by sending a message to the registered mobile number. Merkle tree records the distribution of the block. It is more secured using one-time password authentication and immutable. The result of the system is declared when the polling time is ended. The voting is transparent to the user as a private key is sent to the user to track and view the vote status. The voting can be done anywhere, so the attendance percentage is increased, and even the election results can be declared as soon as the voting process is over.

References
[1] Asraful Alam, S. M. Zia Ur Rashid | Towards blockchain-based E-voting System | 2018.
[2] Fridrik P. Hjalmarsson | Blockchain-based e-voting system | 2019.
[3] Basit Shahzad, Jon Crowcroft | Trustworthy electronic voting using adjusted blockchain technology | 2019.
[4] EIU Democracy Index 2017. Accessed: Aug. 3, 2018.
[5] ScienceDirect. Democracy Online: An Assessment of New Zealand Government Web Sites. Accessed: Aug. 1, 2018.
[6] M. Volkamer, O. Spycher, and E. Dubuis, “Measures to establish trust Internet voting,”
[7] É. Bélanger and R. Nadeau, “Political trust and the vote in multiparty elections: The Canadian case,” Eur. J. Political Res.
[8] T. Kunioka and G. M. Woller, “In (a) democracy we trust Social and economic determinants of support for democratic procedures in Central and Eastern Europe,”
[9] T. van der Meer, “In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics”.
[10] D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, “Election security and economics: It’s all about eve.”
[11] P. Bevelander and R. Pendakur, “Electoral participation as a measure of social inclusion for natives, immigrants, and descendants in Sweden.”
[12] S. Wolchok et al., "Security analysis of India's electronic voting machines."
[13] R.L.Rivest, “The three ballot voting system.”
[14] J.Sten.Votem-Voting for a Mobile World.
[15] M. Pilkington, “11 Blockchain technology: Principles and applications,” in Research Handbook on Digital Transformations.