Blockchain based Transparent E-Voting System

Vaishali Bhorde , Snehal Yadav , Sonal Manwar , Srushti Parit , Prof. Rahul Ghode

1 Vaishali Bhorde,Information Technology,DPCOE Pune,Mahrashtra ,India
2 Snehal Yadav ,Information Technology,DPCOE Pune,Maharashtra,India
3 Sonal Manwar ,Information Technology,DPCOE Pune,Maharashtra,India
4 Srushti Parit , Information Technology,DPCOE Pune,Maharashtra,India
5 Prof.Rahul Ghode, Information Technology,DPCOE Pune,Maharashtra,India

ABSTRACT

The voting or election process is one of the most important and crucial realizations that have been utilized increasingly all over the world in democratic countries. There are very few countries that are based on dictatorship and monarchies nowadays and most of these countries also perform elections in one way or another. There are also elections that are performed in the corporate environment and in municipalities of cities and other jurisdictions. This is the reason why most of the effective and useful mechanisms for the realization of the public opinion are based on the practice of voting. Voting ensures that the voice of the people is heard and they also have a say in the various implementations that affect them. But the process of voting has been unchanged since millennia, there have been numerous advancements in various fields and the technology has been improving every year. The most common issue with modernizing the voting mechanism is the lack of security for the post voting data. Therefore, to solve this drawback, this research outlines an effective and useful mechanism for the securing of the post voting data using the distributed ledger system called blockchain. The standalone application for voting has been designed that maintains the integrity of the data through blockchain which has also been quantified using experimentation the results of blockchain performance.

Keyword : - *E-Voting, blockchain ,Block heads, Terminal Key, Key Evaluation*

1. INTRODUCTION

Voting as a means of decision-making is a representation of organizational and political democratization. Owing to its accessibility, speed, ease of involvement, and cheap expense, electronic voting has been included into many decision-making circumstances with the advancement of networking technologies. Prior to this, academics presented the very first e-voting technique that achieved the goal of an electronic elections by including properties like constitutionality, confidentiality, non-repeatable, tamper-resistant, and so forth. The existing e-voting procedures, meanwhile, have a single administrator who oversees the entire election system. Due to the management's deception, this option would result in rigged election, and there are currently no simple solutions. As just a revolutionary platform for electronic voting, the decentralized blockchain may be used to circumvent the centralized authorities.

The blockchain comprises a decentralized network comprised of numerous interlinked servers that functions as a decentralized distributed ledger system. Additionally, every node within the system has its own public blockchain that is where the transaction information that have already been verified by the blockchain are stored. Somebody with remote access is capable of accessing the data in this ledger. Consequently, all nodes inside the blockchain technology monitor and preserve this chain. The transaction is recognized and stored within every node's distributed ledger whenever the majority of nodes reach consensus, making it impossible to change the transparent and inclusive. All authorized nodes have had the capacity to examine the information captured throughout the voting procedure and the consequences since it is stored on the blockchain.

For making voting increasingly equitable and accessible, all stakeholders work collaboratively to monitor the electronic voting system. Public networks, alliance channels, and private channels are types of blockchains. The plan is designed to be implemented on the private blockchain since it may be used in circumstances involving small-scale campaigns. Every transaction involves a voting procedure, and every transaction generates a new block. This strategy guarantees impartiality and openness not only during the electoral system as well as the election results. Additionally, the blockchain architecture offers node confidentiality, which may be employed in electronic voting to enable anonymized voting.

1.1 RELATED WORK

Due to its decentralized structure and resistance to data tampering, ledger has shown to be a helpful tool in actual situations, although Quang Nhat Tran [7] notes that there are currently some unanswered questions about data accessibility and participant confidentiality. Strategies to preserve confidentiality should be used in mind when creating the potential of blockchain technology while sacrificing privacy. Researchers have covered the existing difficulties with information privacy while using blockchain in many industries in our study. Depending on that, researchers reviewed certain significant advancements in various blockchain's practical fields before classifying the forms of anonymity in accordance, providing two tiers of classification for private information block chain technology.

According to Ali Benabdallah [10], Blockchain looks to be an intriguing replacement for conventional voting methods. The blockchain industry is a continually changing environment as new entities enter whereas everyone else go. In fact, a growing number of research papers in the academic papers suggest blockchain-based electronic voting possibilities. However, only a handful of suggested remedies have really been put into practice, and neither have undergone extensive testing. Consequently, it is quite challenging to draw the conclusion that blockchain today offers a completely secure substitute to holding a democratic election. Despite the security of the blockchain's underlying assumptions, a number of assaults can still target e-voting software. This makes it incredibly difficult to ensure an election's authenticity, which is tantamount to saying that the election has been compromised.

A blockchain-based election mechanism is proposed by Muhammad Shoaib Farooq [13] in order to increase voter confidence in the administration and ensure the security of their election process. Voting on the blockchain also makes the procedure accessible and reliable. The cost of voting in any nation is quite expensive when utilizing the old voting method, but the suggested alternative would use blockchain ballot technology to render voting simpler, quicker, and more reliable. People's relationships towards the democratic country are improved as a result since they have a systematic framework they can depend on. In order to raise the integrity of the election system and increase its dependability, accountability, and confidence, the architecture discusses on the characteristics, capabilities, and responsibilities of respective authority utilizing blockchain inside the electoral system. Each vote is verified, making the results immutable. The notion of publicly and personal keys enables the administration to accurately control the procedure while the usage of hash ensures the anonymity of participants.

2. PRAPOSED METHODOLOGY

The presented approach for the purpose of enabling effective security of the post voting data through the use of blockchain has been defined in the system overview diagram below.

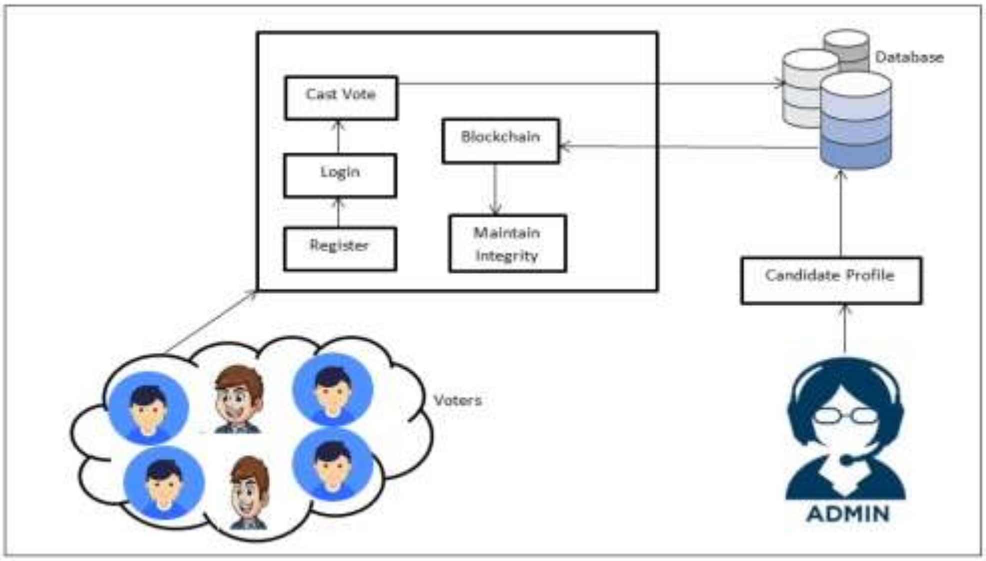

Figure 1: Proposed model System Overview

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work. The subsequent steps for achieving this methodology have been listed below

Step 1: Admin Login and Candidate Profile creation –

In this initial stage of the suggested process, the interactive design is built in the form of a standalone application utilizing the swings framework in Java. After logging in, the administrator may utilize the manage candidate option to add names to the list of those who can run for office. The manage candidate menu consists of 3 different sub menus, namely, add candidate, view candidate, and delete candidate. To perform the candidate profile creation the admin will select the add candidate sub menu. The admin then adds the various details of the candidate such as name, age, sex, qualifications, worth, profession, Constituency, symbol name, symbol image and party name. Once these details are added, the admin clicks on save and the candidate is added to the database. This is performed for all the candidates that are standing for the election.

Step 2: Voter Registration–

The admin are in charge for the creation of the voter profiles using the swings standalone application to access the service. Before granting access to the voter, the voter must submit login information which are already validated. These details include, name, father name, age, sex, date of birth, Aadhar number, email id, mobile number, address, and state. Once these details are collected, the admin can access the voter menu in their operation frame and select the add voter sub menu to create the voter account using the provided information. Once the voter is created the voter profile can be used for casting the votes in the next step.

Step 3: Voting process–

The voting process starts from the vote menu on the admin profile, the admin is tasked with the selection of the start sub menu in the vote menu. Once the voting process page is accessed by the admin, he/she has to select the constituency where the voting process is being initiated. Once the constituency is selected the already registered voters from the same constituency need to provide their Aadhar number into the system. The email linked to the Aadhar number and voter profile is then sent an email with an OTP for verification. Once the user authenticates with the OTP the list of the valid candidates for that particular constituency are listed to the voter with their names and party symbols. The voter can then select the candidate of his/her choice and click on vote to cast the vote. The votes are secured by encrypting them and converting it into a blockchain which will be discussed in the next step.

The admin after logging into the system, the voter is provided with a list of contenders and their biographies organized by political organization or allegiance. The electorate can next pick among candidates affiliated with their preferred political party. The voter's decision, coupled with the Aadhar card information, is acknowledged when the candidate is chosen, and the Blockchain infrastructure is activated.

Step 4: Blockchain Formation –

An effective method of demonstrating accountability after the vote has been awarded to the candidate is necessary in an effort to discourage vote manipulation. Thus, the Blockchain was built to accommodate this requirement. The voter's Aadhar number is collected at the time of the first vote on the suggested technique. The MD5 hashing method is used to produce the vote's key. The specific character from this Hash key is selected to form the Head key. Because of this, the Head Key is the name often given to this particular key. In algorithm 1 we see how the keys are generated.

Step 5: Data Integrity through Blockchain–

When every voter has cast their ballot, the administrator must stop accepting ballots. The administrator has to select the close voting option and provide a valid email id in order to end the voting process. Sending the blockchain's terminal key to that address will be the next logical step. At this stage, we utilize the terminal key received in the admin email in conjunction with the input text from the database table where the vote was placed. After that, the MD5-bit hashing algorithm is used to create the hash. To determine a practical length for the keys, the hash key rotations as well as random character picking are used to narrow down the pool of potential candidates to a manageable size.

The beginning and end blocks of a block chain are acquired at some point. The whole set of voting results from the application is going through this process again so that we may get the master key. During an integrity examination, both the current and prior master keys are available for inspection. While comparing the current and previous head keys, discrepancies are identified as potential integrity violations, and an alarm is triggered if one is present.

2.1 ALGORITHMS

Algorithm 1: Block Head Key Generation

```
// Input:  Vote Attributes $V_A$
// Output: Head Key $H_K$
Function: headKeyGenerator ($V_A$)
Start
$H_K = Ø$
$H_{KEY} = MD5\ (V_A)$
$HK = H_{KEY[0]} + H_{KEY[5]} + H_{KEY[11]} + H_{KEY[14]} + H_{KEY[23]} + H_{KEY[26]}$
return $H_K$
Stop
```

Every time a new round of votes is cast, the very same parameters are calculated and added to the previous transaction's head key, and the whole hash key creation procedure is performed using MD5 to produce the following transaction's head key. This is repeated for every eligible voter, and the final operation or vote is secured by the terminal key, which is stored in a separate database for confidentiality. Algorithm 2 below depicts the process of creating a blockchain.

S. No	No. of votes/ Blockchain	Time Taken (in seconds)

ALGORITHM 2: Blockchain Formation

```
//Input : Vote Information list $V_L$
//Output: Terminal Key $T_K$
blockchainFormation($V_L$)
Start
$P_K$ =” ” [Previous Key]
  for i=0 to size of $V_L$
    $T_{PL}$=$B_{L[i]}$ [$T_P$ = Database Tuple]
    $P_{KEY}$= getBodyKey($T_{PL}$)
    $T_K$ =$P_K$
  end for
  return $T_K$
Stop
```

3. RESULT AND DISCUSSIONS

The proposed method was developed using the Java programming language and the NetBeans IDE to streamline the process of electronic voting with the help of Blockchain. The Windows OS-running development machine has 4 GB of RAM and 500 GB of hard drive space available to it. MySQL is in command of all database administration.

The efficacy of the proposed strategy was assessed across a number of criteria. Here, you will find a summary of the results of the empirical study.

3.1 Scalability Analysis of Blockchain Transaction

The proposed method for protecting voter information and its validity through Blockchain is used to evaluate the scalability of Blockchain transactions. To achieve this objective, a number of different lines of exploration are being pursued, among which is the development of a safe and reliable interactive interface for the voting procedure. The number of transactions and accessible operations on the Blockchain is shown in Table 1.

1	**256**	**0.512**
2	**541**	**1.005**
3	**801**	**1.764**
4	**965**	**2.004**
5	**1299**	**2.217**

Table 1: Blockchain Transaction Time Estimation Table

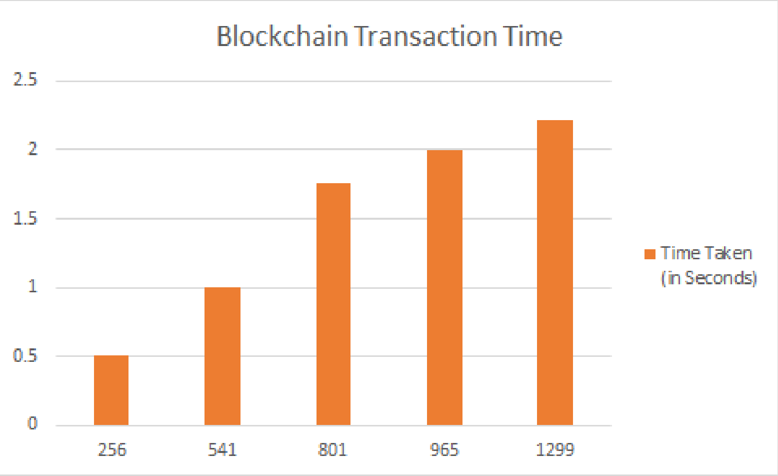

Figure 2: Blockchain Transactions Time

Figure 2 is a graph generated using the tabular findings. The graph has been useful in demonstrating the correlation between the number of Blockchain network operations as well as the time needed to execute them. The study's findings shed light on the methodology and how Blockchain technology could be put to use to protect the privacy of voters' personal information throughout the voting process. It is obvious that the time required to conduct a transaction on the Blockchain is disproportionate to the number of votes cast or the number of operations performed. That demonstrates that the Blockchain strategic approach succeeded as intended. The results helped shed light on why voting has become more secure as a whole.

4. CONCLUSIONS

One of the most significant and critical realizations that has been used more frequently in democratic countries across the world is the voting or election process. Nowadays, dictatorships and monarchies are relatively rare, and the majority of these nations still have elections in some form or another. Additionally, elections are held in the business world as well as in municipalities of cities and other authorities. This explains why voting is the foundation of the majority of useful and successful procedures for realizing public opinion. Voting guarantees that the public's voice is heard and that they have a say in the policies that impact them. However, despite innumerable scientific discoveries and technological improvements, the voting process has not altered since the dawn of time. The absence of security for the post-vote data is the most frequent problem with upgrading the voting system. As a result, this research presents an efficient and practical solution for the post vote data security utilizing the distributed ledger technology known as blockchain. A web application for voting has been created that uses blockchain to ensure the data's integrity. The effectiveness of this system has also been assessed through experimentation, and the findings are discussed in more detail in the following sections

5. REFERENCES

1] R. P. Pinto, B. M. C. Silva and P. R. M. Inácio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain," in IEEE Access, vol. 10, pp. 92760-92773, 2022, doi: 10.1109/ACCESS.2022.3203193.

[2] I. Malakhov, A. Marin, S. Rossi and D. Smuseva, "On the Use of Proof-of-Work in Permissioned Blockchains: Security and Fairness," in IEEE Access, vol. 10, pp. 1305-1316, 2022, doi: 10.1109/ACCESS.2021.3138528.

[3] C. Santiago, S. Ren, C. Lee and M. Ryu, "Concordia: A Streamlined Consensus Protocol for Blockchain Networks," in IEEE Access, vol. 9, pp. 13173-13185, 2021, doi: 10.1109/ACCESS.2021.3051796.

[4] H. Guo, W. Li, M. Nejad and C. -C. Shen, "Proof-of-Event Recording System for Autonomous Vehicles: A Blockchain-Based Solution," in IEEE Access, vol. 8, pp. 182776-182786, 2020, doi: 10.1109/ACCESS.2020.3029512.

[5] W. She, Q. Liu, Z. Tian, J. -S. Chen, B. Wang and W. Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 38947-38956, 2019, doi: 10.1109/ACCESS.2019.2902811.

[6] Y. Bai, Q. Hu, S. -H. Seo, K. Kang and J. J. Lee, "Public Participation Consortium Blockchain for Smart City Governance," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2094-2108, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3091151.

[7] Q. N. Tran, B. P. Turnbull, H. -T. Wu, A. J. S. de Silva, K. Kormusheva and J. Hu, "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture," in IEEE Open Journal of the Computer Society, vol. 2, pp. 72-84, 2021, doi: 10.1109/OJCS.2021.3053032.

[8] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro and R. Sharma, "An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions," in IEEE Access, vol. 10, pp. 116858-116906, 2022, doi: 10.1109/ACCESS.2022.3219160.

[9] S. Gao, D. Zheng, R. Guo, C. Jing and C. Hu, "An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function," in IEEE Access, vol. 7, pp. 115304-115316, 2019, doi: 10.1109/ACCESS.2019.2935895.

[10] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 70746-70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[11] G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[12] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in IEEE Access, vol. 7, pp. 24477-24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[13] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in IEEE Access, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168