Enriching E-voting process through Blockchain on Web Applications

Amay Sandanshiv
Vivek Salve
Tejas Muthe
Sameer Shaikh
Prof. Balaji Bodkhe

Computer Engineering Dept., MESCOE, Pune.

Abstract

A democratic democracy is defined by honest and impartial elections. The primary goal of a democratic society is to organize elections in a stable and secure way, which is a key duty for different authorities. With an increasing number of voters and a large number of polling places designed to help everyone who has reached the legal voting age in casting their ballot, the majority of the inspectors tasked with overseeing these elections have been put under strain. In charge of conducting functional elections, every one of these votes from individuals should always be obtained. As a consequence, the Blockchain architecture is being proposed as a way to increase vote security whilst simultaneously cutting election costs. The blockchain is among the most reliable technologies for ensuring tamper-proof results due to its robust construction. The results of earlier studies have shown to be useful in deciding on a blockchain technique for efficiently safeguarding post-voting information. In future revisions of this study piece, this technique will be expanded upon. As a result, this research work uses Blockchain to give a secure solution to ensure protection for post-voting data in a regulated simulated environment. The hash keys of 16-byte generated by the SHA 256 hashing method and Bit mapping mechanism fuel the entire operation.

Keywords— *Blockchain, E-Voting, SHA 256, Bit mapping*.

I. INTRODUCTION

Democracy is undoubtedly the most extensively utilized and effective technique of government on the planet. The core motto of democratization is an extremely important statement considering democracies organize elections wherein residents vote for politicians to govern the country. This is an extremely significant aspect of the nation because the administration is responsible for a range of rules and regulations governing the citizens' daily life. The elected politician is a permanent resident who has been appointed to administer people freely by the public.

As a consequence, democracy is a magnificent program that gives inhabitants of a country authority. Since in a democratic state, the capacity to vote would be both essential and crucial. Elections and ballot procedures are, without a doubt, among the most important events in a modern democracy. Elections are a long and difficult undertaking that is handled by the electoral commission, an impartial, non-governmental entity (EC). The Election Commission is already in responsible for directing the many factors that go into running a fair and honest election.

The very first step in the extensive election process will be to identify different voters, which also will continue to go up each year as more people reach legal age. This database must be refreshed ahead to the election, and the election commission does it by physically inspecting individual homes to identify and authenticate the many voters. When the electoral register is modified, the electoral commission must arrange for the election by establishing voting booths in each constituency. The constituency is defined by the members and demographics of the province.

When polling locations are constructed, the population density is taken into account to ensure that residents are not impacted.

In India and several other nations, electronic voting machines, or EVMs, are used to execute elections. The purpose of these gadgets is to keep track of the various votes cast by the participants. The polling booths originally designed with the number of persons who could really vote in that particular constituency in consideration, both to alleviate congestion and to aid law enforcement in preserving law and harmony.

To ensure that everybody has the potential to vote, the polling day is declared a holiday. This can also be attributed to the fact that some citizens travel long distances to vote in their constituency on Election Day. From law enforcement officers manning voting booths to people employed to manage the myriad duties and documents needed to ensure that the elections are handled correctly, the election commission invests a significant amount of money to ensure that the polls function smoothly and successfully.

The polling stations are entered on Election Day, but all of the votes from around the country are assembled and put in a closed container. Professionals from each political party scrutinize the countless sealed ballot boxes for anomalies or errors. These boxes, which contain eligible voter ballots, are brought to a secure location on Election Day, where officials count the votes for each constituency. Following that, the ballots will be utilized to build a list that is categorized in ascending order, accompanied by the winner's declaration.

Calculating the various votes and accurately and quickly displaying the results is a time-consuming process that can be prone to error. The results can be significantly influenced and sensitive to a number of attacks because the counting is done manually and individual mistakes are easily included. Understanding of the physiological essence of votes, there is a significant possibility of tampering, as well as certain ballots are destroyed completely during the phase transition or go unnoticed in every election. The ballot can be opened before the tallying period begins, and if it is, it will be considered manipulated and eliminated from the final result. Something like this would jeopardize the election committee's efforts to proceed.

Physical ballots are an out-of-date method that really should be eased away. Since this Digital India program gathers traction in the country, the implications of an E-Voting system must be investigated. This type of technology might make voting processes more efficient and comfortable for voters. People might vote digitally using an E-voting system, removing the need for a polling location and the time-consuming physical method. Decreased voting booths would decrease wastages while also increasing voter turnout, which had been quite low before the election but has been steadily increasing since then. The advantages of transitioning to electronic voting are considerable, but for many people, the problem of security is the only deterrent.

II **Literature Review**

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

X. Yang et al. [1] present a voter-verifiable e-voting system that allows voters to cast ballots by allocating arbitrary quantities of points to various candidates. This implies that voters can give each candidate the same nuber of points, or they can give each contender a different number of points. The distributed ElGamal cryptosystem is used in the system. Before being submitted, each cast ballot is encrypted and stays encrypted at all times. The exponential ElGamal cryptosystem's additive homomorphic characteristic allows for efficient ciphertext processing throughout these processes. Furthermore, anybody may check the legitimacy of voters and their submissions without revealing the contents of the ballots.

S. Bartolucci et al. provide options for announcing and building an election, as well as determining a victorious candidate, utilizing blockchain technology. The authors focus on how to broadcast and accurately count votes within the transactions script while maintaining voters' privacy and anonymity, enabling only eligible users to vote, and avoiding attacks aimed at invalidating the ballot [2]. If no candidate gathers enough key shares to spend the UTXO in the transaction signed by the voters, the SHARVOT protocol is built with a failsafe, allowing any Bitcoins committed by the voters to be recovered. Because a dealer assumes the function of an authority control over the list of eligible voters, a dealer-based key share distribution scheme is predicted to be the most popular implementation of the SHARVOT protocol.

Fatrah, Aicha et al. presented a Blockchain-depend voting framework as a proof of concept. The technique intends to promote election transparency, voter confidentiality, and, ultimately, voter turnout by empowering any qualified voter to engage in and audit the system. Election administrators are the ones who issue reward points that permit voters to vote on the blockchain; however, all interactions between election administrators and voters must take place off-chain, and election administrators anticipate that voters will converse with the blockchain through a secure platform [3]. They must include an election date, a candidate list and explanation, and the system's POA validators. Because the offered system is built on Blockchain technology, it contains all of the security characteristics of the blockchain.

X. Yang et al. offer a collection of online social voting RSs depending on MF and NN. The authors discovered that both social network information and group affiliation information can improve the accuracy of popularity-based voting recommendations, especially for cold users, through real-world experiments, and that social network information dominates group affiliation information in NN-depend strategies. This research found that for cold users, social and group information is far more valuable than for heavy users when it comes to enhancing recommendation accuracy [4]. This is because chilly users are more likely to vote in popular polls. In the tests, simple meta path-depend NN models outperformed computation-intensive MF models in hot-voting suggestion, although MF models can better mine users' interests for nonhot voting.

To recognize and address the numerous hazards produced by an intruder at multiple levels, Blockchain technology was employed by G. Rathee et al. to establish a safe and transparent e-voting mechanism using trustworthy IoT devices. The trustworthiness of IoT devices is determined by a social optimizer that analyses their communication patterns to determine their trustworthiness. Furthermore, in the suggested system, Blockchain technology is critical for coordinating the operations of genuine IoT devices [5]. Blockchain is maintained at several levels to keep track of all the recorded information handled by election conducting bodies to prevent a potential alteration of stored records of votes in databases. The suggested Blockchain voting process benefits not only elected officials but also voters, who are warned if their ballots are tampered with before the planned counting day.

T. Silawan et al. offer the SybilVote formulae to address the effect of Sybil attacks in online social networks with majority-voting mechanisms, as expressed by the success probability of Sybil attacks [6]. It's worth noting that the goal of the presented research isn't to figure out who Sybil is, but rather to figure out how Sybil attacks work. The SybilVote algorithms developed here quantify the direct link between the number of genuine users, choices, and Sybil users. The consequent multinomial distribution of vote counts from non-Sybil users is the sole assumption required. By comparing the generated formulae to Monte-Carlo simulations and the multinomial distribution tail approximation formula, the formulas are assessed.

T. Tian et al. present a simple and straightforward maximum margin majority voting estimator for learning-from-crowds, as well as its Bayesian version, which combines generative modeling with discriminative prediction [7]. The presented approaches automatically cover the traditional Dawid-Skene estimator since they are formulated as a regularized Bayesian inference issue. The efficiency of their approaches is demonstrated by empirical outcomes. Their approach is adaptable to a variety of complex application scenarios. They improve the estimators to better handle crowdsourced labels having an ordinal structure. When additional jobs are spread, Bayesian estimators are extended to the online environment, where the crowdsourced labels are gathered in a stream.

Yi Haibo describes a blockchain-depend e-voting approach that satisfies the indispensable requirements of the e-voting process. The blockchain's votes are cryptographically connected block by block. When two blocks with the same date and the same signature value are found, the block with the higher signature value is picked. The voter may vote based on the candidate list or for any other candidates he or she desires [8]. Because the vote is usually available to the public, the information concerning the vote is not encrypted. The blockchain-depend e-voting system may be utilized in a diversity of voting scenarios as well as for other reasons. Even though blockchain is a secure technology, it uses ECC public-key encryption, which is vulnerable to quantum computer attacks.

Ben Ayed [9] proposed an electronic voting mechanism based on Blockchain technology. It's a decentralized system with no reliance on trust. Any registered voter who has access to the Internet will be allowed to vote. The user must log in to the voting arrangement with his or her credentials—in this case, the e-Voting network will employ the user's SSN, address, and the voting verification numbers given to registered voters by the local authorities. The system will verify the information provided, and if it matches that of a valid voter, the user will be permitted to vote. Because the Blockchain will be openly validated and disseminated, no one will be able to modify it.

Fusco et al. provide a research proposal for defining and implementing a novel electronic voting system idea [10]. Crypto-voting is a voting mechanism that depends on permissioned blockchain technology. When compared to the state of the art, the factors of innovation include the strategy, the technology, and the usage of tools like Smart Contracts. The proposal focuses on the sidechain technology's potential. The authors discussed how two connected blockchains may be used to construct a crypto-voting system. The first keep track of voters and voting procedures, while the second count the ballot and reports the results. The need for anonymizing network consensus nodes is emphasized in this technique. The voting procedures and outcomes will be managed via smart contracts.

A decentralized voting platform depending on the Ethereum Blockchain has been suggested by D. Khoury et al. The platform's key contribution is the ban on numerous votes per mobile device. Depending on fingerprints or a particular gadget situated in voting centers, this technique might be improved to build it more suitable for national government elections [11]. The user articulation and results display might be tailored to the needs of the customer. This platform might replace existing centralized SMS polling systems and make voting easier for governments, contests, and expositions, among other things. This platform introduces a new business framework for voting service providers, including voting service providers, event organizers, and voters as participants.

D. Khoury et al. give a recapitulation of the computerized voting technique. This includes identifying the polling process, selecting the appropriate hash algorithm, selecting blockchain changes, the process of voting data management, and the security and authentication of the voting operation in particular. The polling method described in this research depends on the real voting procedure utilized on election day, which involves physical and logical verification of the voter and the voter's data, but solely through the use of voter lists and other information [12]. The computerized voting procedure ensures that voters may be verified using their physical records, such as a national identity card, as well as biometric authentication. The verification system's availability during polling time is critical because the procedure cannot be completed without a fully operational system.

F. Þ. Hjálmarsson et al. presented a first-of-its-kind blockchain-depend electronic voting framework that uses smart contracts to dispense cautious and cost-effective elections while protecting voters' privacy. By comparing the findings to previous research, the authors have demonstrated that blockchain technology provides a new opportunity for democratic countries to move away from the pen and paper election system and toward a more cost- and time-effective election system, while also improving security and transparency [13]. It is feasible to transfer hundreds of transactions per second into an Ethereum private blockchain, employing every component of the smart contract to reduce the load on the blockchain. For larger nations, various precautions must be made to limit transaction throughput per second, such as the parent & child architecture, which decreases the number of transactions kept on the blockchain to a 1:100 ratio without jeopardizing the security of the network.

III PROPOSED SYSTEM

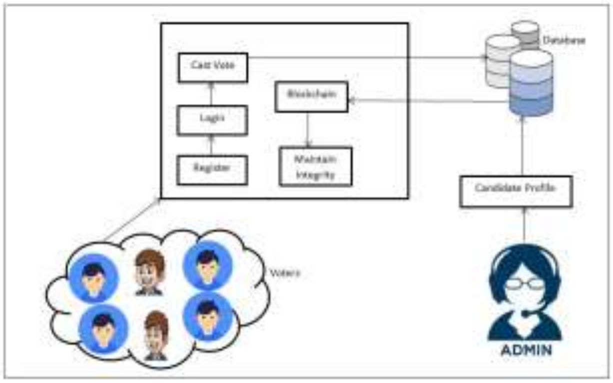


Figure 1: System Overview

The proposed approach for safeguarding the election's post-voting records is represented in Figure 1 above, and the procedures taken to implement it are described below.

Step 1: *Candidate Profile creation* – The interactive prototype is constructed in the format of a web application in this first part of the suggested concept. After authenticating into the system, the administrator is provided the opportunity to register election contenders. The party name, emblem, contestant name, age, sex, and other needed qualities to save in the database are among the candidacy data input in the given graphical interface. After all of the candidates have been registered to run for office, the voters begin the election process.

Step 2: Voting process and Blockchain formation – Participants can also use the web application to access the service. Before granting access to the voter, the voter must submit login information which are already validated. 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.

In attempt to deter vote manipulation, an appropriate means to establishing some form of responsibility once the vote has been granted to the candidate is required. As a consequence, the Blockchain architecture was developed to meet this need. When the first vote on the proposed approach is submitted, the voter's Aadhar card number is obtained. The key for this vote is generated using the SHA256 hashing algorithm. The key generated using this approach is then changed into a shortened key using the mod operation, which selects 7 characters at arbitrary from the key. As a result, this key is known as the Head Key. The key generating technique is described in algorithm 1 below.

Algorithm 1: Block Head Key Generation

```
// Input:  Vote Attributes $V_{ATR}$
// Output: Head Key $H_K$
Function: headKeyGenerator ($V_{ATR}$)
Start
$H_K$ =Ø
  $SH_{KEY}$=SHA256 ($V_{ATR}$)
      N=$SH_{KEY}$ MOD 7
    If N<7, then
    P=N+1
            for i=0 to $H_K$ length < 7
                i=i+P
                if i < $H_K$ length, then
                    $H_K$ = $H_K$ + $SH_K$ [i]
                    $SH_K$ = rotate ($SH_K$)
                end if
        else
                i=0
            end for
      end if
return $H_K$
Stop
```

The very same parameters are determined and combined with the previous transaction's head key whenever the next votes have been cast, and the entire hash key construction operation using SHA256 is performed to generate the subsequent transaction's head key. This is replicated for all registered voters, and the terminal key, which would be maintained in a separate database for privacy reasons, is the key of the final transaction or vote. The procedure of forming a blockchain is depicted in algorithm 2 below.

ALGORITHM 2: Blockchain Formation

```
//Input : Vote Information list $V_{LST}$
//Output: Terminal Key $T_{KEY}$
blockchainFormation($V_{LST}$)
Start
$P_K$ =” ” [Previous Key]
```

```
for i=0 to size of $V_{LST}$
    $T_{PL}$=$B_{L[i]}$ [$T_P$ = Database Tuple]
    $P_{KEY}$= getBodyKey($T_{PL}$)
    $T_{KEY}$ =$P_{KEY}$
end for
return $T_{KEY}$
Stop
```

Step 3: Data Integrity through Blockchain– This phase makes use of the stored vote's input string from the database table. The hash is generated using the SHA 256 bit hashing technique after that. Random characters are shortlisted utilizing the hash key rotations and random character choosing to establish the reasonable length of the keys.

Eventually, the block chain's block head and block body are obtained. This procedure is being repeated for all of the application's voting results in order to obtain the final head key.

Present and previous head keys are exposed to the integrity evaluation procedure during the integrity assessment process. Whether there are any inconsistencies between both the current and prior head keys, the integrity breaches are discovered and the necessary alert is generated.

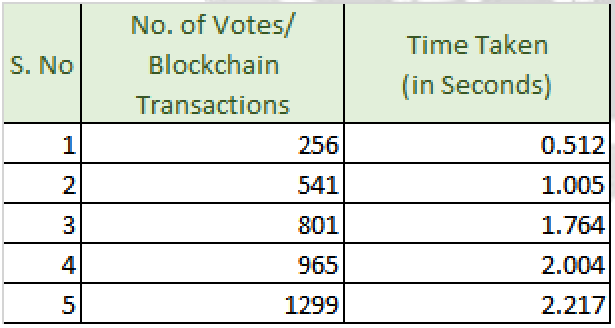
IV RESULT AND DISCUSSIONS

The described approach, which uses the Java programming language and the NetBeans IDE to simplify electronic voting through the usage of Blockchain, was created utilizing Java programming language and the NetBeans IDE. For webhosting, the web application makes use of the Glass Fish web server. The developing computer is furnished with a Windows Operating System, 8 GB of RAM, and 500 GB internal memory. The MySQL database is in charge of database management.

The suggested approach has been thoroughly evaluated for its effectiveness over a wide range of criteria. The outcomes of the empirical examination are listed beneath.

Scalability Analysis of Blockchain Transaction

The scalability of Blockchain transactions is determined using the given approach for safeguarding voter information and its authenticity through the Blockchain. An extensive investigation is being carried out for this goal, which includes the construction of a secure online interface for the voting process. Table 1 shows the volume of Blockchain transactions that have been recorded and displayed.



S. No	No. of Votes/ Blockchain Transactions	Time Taken (in Seconds)
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

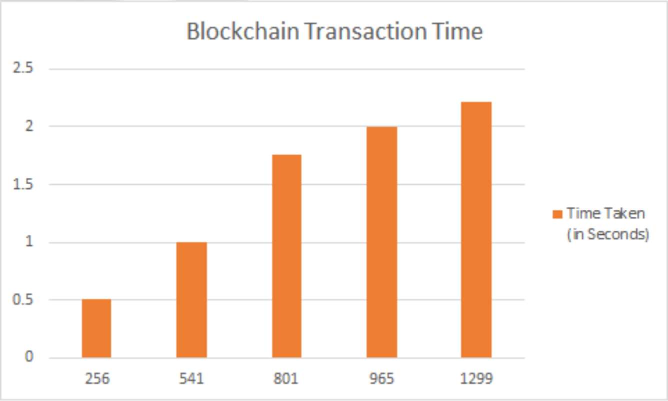


Figure 2: Blockchain Transactions

The tabular results are then utilized to create the graph seen in Figure 2. The graphical depiction has shown to be successful in illustrating the link between the quantity of operations and the time required to complete them on the Blockchain network. The results of the analysis offers a better knowledge of the methodology and the use of the Blockchain architecture to ensure the vote data's confidentiality. It is clear that the variety of votes or Blockchain operations is not proportionate to the amount of time it takes to complete the transaction. This shows that the Blockchain strategy was correctly implemented. The findings were useful in explaining the increased security of the entire electoral process.

V. CONCLUSION AND FUTURESCOPE

This study effectively implements the procedure of E-voting in a web application utilising the Java programming language in a well-organized and structured manner. To protect E-Voting data, the suggested model makes use of the Blockchain Network, which surpasses a wide variety of standard electronic voting systems by a significant proportion. The whole E-voting data is protected through using block chain technology. The suggested strategy secures the voting data by storing it in blockchains. Through the usage of prior and present terminal head keys, these blockchain transactions are utilised to evaluate the pre-counting operation. The runtime effectiveness of the blockchain procedure is analysed, and it is demonstrated that this is not necessarily correlated to time. As a result, the blockchain surpasses in terms of time sequence estimations when compared to the quantity of transactions. The parallel computation approach used in this research promises to reduce the temporal complexity of the E-Voting information integrity assessment process, allowing it to be properly protected.

This research concept might be expanded in the future to include real-time elections for electronic voting machines at the panchayat or perhaps in larger geographic locations.

a. REFERENCES

[1] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in IEEE Access, vol. 6, pp. 20506-20519, 2018, DOI: 10.1109/ACCESS.2018.2817518.

[2] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARe-Based VOTing on the Blockchain," 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2018, pp. 30-34.

[3] Fatrah, Aicha & El Kafhali, Said & Haqiq, Abdelkrim & Salah, Khaled. (2019). Proof of Concept Blockchain-based Voting System. 1-5. 10.1145/3372938.3372969.

[4] X. Yang et al., "Collaborative Filtering-Based Recommendation of Online Social Voting," in IEEE Transactions on Computational Social Systems, vol. 4, no. 1, pp. 1-13, March 2017, DOI: 10.1109/TCSS.2017.2665122.

[5] 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.

[6] T. Silawan and C. Aswakul, "SybilVote: Formulas to Quantify the Success Probability of Sybil Attack in Online Social Network Voting," in IEEE Communications Letters, vol. 21, no. 7, pp. 1553-1556, July 2017, DOI: 10.1109/LCOMM.2017.2687867.

[7] T. Tian, J. Zhu, and Y. Qiaoben, "Max-Margin Majority Voting for Learning from Crowds," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 10, pp. 2480-2494, 1 Oct. 2019, DOI: 10.1109/TPAMI.2018.2860987.

[8] Yi, Haibo. (2019). Securing e-voting based on blockchain in the P2P network. EURASIP Journal on Wireless Communications and Networking. 2019. 10.1186/s13638-019-1473-6.

[9] Ben Ayed, Ahmed. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. DOI: 10.5121/ijnsa.2017.9301.

[10] Fusco, Francesco & Lunesu, Maria Ilaria & Pani, Filippo & Pinna, Andrea. (2018). Crypto-voting, a Blockchain-based e-Voting System. 223-227. 10.5220/0006962102230227.

[11] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018, pp. 1-6, DOI: 10.1109/IMCET.2018.8603050.

[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] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, DOI: 10.1109/CLOUD.2018.00151..

*****