IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.2, February 2021 E-ISSN: 2347-2693

Online Voting System Based on Blockchain

B.T. Prasanna[1*], Rakshitha R.[2]

[1,2]Department. of Computer Science and Engineering., JSS S&TU Campus, Mysore, Karnataka, India

**Corresponding Author: prasannabt@jssstuniv.in*

DOI: https://doi.org/10.26438/ijcse/v9i2.6064 | Available online at: www.ijcseonline.org

Received: 20/Feb/2021, Accepted: 25/Feb/2021, Published: 28/Feb/2021

Abstract— Voting plays an important role in making decision and is an serious event as it determines the fate of a nation. In Current voting System, voters cast their vote in an appointed polling stations, which usually involves more expenditure on time and cost budget. In this paper aiming to implement the application of Blockchain as a service to implement distributed Online Voting Systems. Blockchain based Online Voting System (BOVS) to enhance the integrity, optimize the voting process, produce consistent voting results, strengthen the transparency of the voting system and and it doesnot allow duplicate votes and is fully tamper proof. In this System voting is convenience to users as voters can vote from their devices without extra cost and effort. In this paper we explore the advantges of Online voting system based on Blockchain technology.

Keywords— Voting, distributed, transparency, tamper proof, Blockchain.

I. INTRODUCTION

In every democracy, The national security is ensured by conducting the election process securely. Election is the process to collect the public interest to form a republic government. The election process should be transparent, reliable and provide option for people to vote online without compromising on security. In Current Voting system , the votes are read and counted manually by Booth manager from each EVM and sum them to get overall vote count casted for the candidate[1]. This System might cause ballots to be done fraud and ballots failure might cause; ballots can be miscounted, or ballots sent via mail might get lost on the way and a huge amount of money is required during every election in a country.

The internet has been evolving rapidly, and has greater effect on our daily lives, hence there must be a option for the people to cast vote online without compromising on security. Through Online voting or E- voting, the entire voting process is completed at a minimal cost and speed. The time taken for conducting the election process is reduced, it will greatly enhance the efficiency of the government and voting process is verifiable and recoverable [2].

Electronic voting (e-voting) can be defined as employing electronic means or information technologies to conduct voting process. Every e-voting system consists of registration, authentication and authorization, vote casting, vote counting and vote verification. Voters can vote from anywhere placed in different locations, can take part in the election process and participate in election process. When voter cast votes, every vote is added to block as transactions, and a Blockchain is created which keeps track of all casted votes. The final aggregate count of votes is obtained by counting the transactions blocks of Blockchain , Votes are managed such that no votes are changed or removed, and no duplicate votes were added.

Electronic voting or Online voting provides higher security by using Blockchain technology. Blockchain is one of the prominent technologies by making use of strong cryptographic functions. Blockchain is used in several fields such as IOT, and various devices are connected to internet, and each and every devices will process different data using new approaches.

A Blockchain is a data structure starting from its genesis block will maintains and shares all the transactions blocks. It is a distributed decentralized database that maintains a complete list of constantly generating and growing data records, it is secured from unauthorized being manipulating, or tampering the records and recover of data is possible . Blockchain connects all user to the internet, send, verify and create new transactions as blocks to Blockchain. Each block is containing a hash value that remains valid in the blocks as long as the data is not being altered. If any malicious attack changes are made in the block, the hash value will change immediately indicating the change in the data . Therefore, due to its strong functions implemented in cryptography, Blockchain has been considerably used to correct from unauthorized transactions across various sectors.

Our main contribution in this paper is 1) Identifying the importance of Electronic/Online Voting System 2) Exploiting different stages or phases involved in election process 3) Understanding how Blockchain service is used

for Electronic/online voting system 4) Results of the System is evaluated.

This paper is organized as follows. Section 2 describes the Related Work. In Section 3, we discuss about the Proposed Method in more detail. Section 4, Results are analyzed in section 5. Finally, we concluded work and discuss the future work.

II. RELATED WORK

The Current System, electronic votes machines (EVM) will be utilized which stores the votes. It isn't associated with web. The Booth manager has to manually tally vote from each EVM and aggregate them to get total vote polled for the candidate. This existing systems are susceptible to attacks and are easily modifiable, Not trustable or very difficult to maintain and has no transparency for vote casting process.

Many research has been made to transfer data securely through network, and numerous strategies have been proposed and actualized for giving Online voting .This Online/Electronic voting System"(EVS) can cast votes, secure them and check the votes during result day. It is associated with the system connected to the internet. The information is moved all more safely through this system.
In 2007, Estonia became the first and foremost country to permit utilization of internet casting a ballot. In 2015 parliamentary elections 30% of votes were casted through e-casting a ballot framework . Estonia uses the national ID card for voters to verify voter. These cards contain the identify data in encoded way. For casting a ballot, the residents can enter their card into a card reader for confirmation. After confirmation the voter gains admit to the voting site on the connected PC . After confirming user details, a voter has access to the voting site for four days. In the wake of checking client accreditations, a voter approaches the site for four days. After submitting the vote, it passes through forwarding server and stored in a server in encrypted form. After the online voting period is completed, these casted votes are transmitted to a counting server which is disconnected from network. This server is responsible for talling the votes and providing the results.
The A. Singh and K. Chatterjee in [3], proposed a model to secure the e-voting system based Blockchain (SecEVS) for the university campus election. was approved during the security examination stage. The proposed system security scheme is based on Merkle root hash. The system kept up the accompanying like Transmitted information protection, Voter privacy, Voter confidentiality, The uniqueness of the polling form which that there are no duplication cases during the voting.

The F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis in [4], proposed bearable new e-voting protocol that used Blockchain as a transparent ballot box. This convention has been proposed to maintain the hidden of e-casting a ballot properties permit a level of decentralization, accommodate the elector to adjust/update their vote inside the admissible voting stage.

The Jason, P. C., and Yuichi, K in [5], proposed E-voting system based on the bitcoin protocol and blind signatures in 2017. They have utilized Bitcoin convention to acknowledge e-casting a ballot system. This system can't ensure the security in some circumstance, for example, if the director realizes the Bitcoin address of the voter, the administrator can know who the voter is by connecting the location and message on the Blockchain.

The Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim in [6],proposed electronic voting service using block-chain in 2016. They propose either a Bitcoin or private Blockchain based approach . Additionally, there is a need for a trusted third party which verifies the voters. voters have to identify their right to vote by proving themselves to both authenticating organization and the trusted third party.

The Yifan Wu in [7],proposed An E-voting System based on Blockchain and Ring Signature in 2017. This system uses basic concept of e-voting and Blockchain by specifying Bitcoin address algorithm and OP RETURN concept. The system does not fulfill the properties of fairness and receipt-freeness. The efficiency of ring signature algorithm is limited by the number of participants..

The Y. Liu and Q. Wang in [8], proposed an e-voting protocol based on the Blockchain without a trusted third party, which affords a safe and adaptable voting technique. This protocol provides Public Verifiability, Individual Verifiability, Dependability, Consistency, Auditability, Anonymity and Transparency.

III.METHODOLOGY

In this paper, we implement Blockchain-based electronic voting systems, we are presenting a novel Secure, Privacy Preserving and cost effective election process concept which uses web-based interface with Cloud Data Storage. In this system Votes are stored securely in Decentralized architecture, transparently in cloud and manipulations of votes are nearly impossible.

The proposed system has three types of people involved in conducting the elections.

a) Admin/ Election officer - An Admin will set the configuration setting required to conduct the election process. The Admin has the authority to add the election date and timings and is responsible to add ,view, edit and delete the election Constituency, Party information, candidates constesting for respective parties, the booth manager in-charge details , register voter's details into the system. The election authority is responsible for tallying the votes. When the voting has been finished, the admin will start counting the votes and announce the results .

b) BoothManager / Incharger - Booth Managers/Incharger are the area manager for each of the constituency. Booth manager will have information about voter details who belong to his booth. He can add or delete any voter from the list. Voters who don't have smartphone will go to the Booth for casting the votes ,where the Booth manager will verify the voter and allow him to poll .

c) Voter - Voter is an individual who is eligible to cast his vote. Each voter will be authenticated and given authority to cast his valuable vote to the desired candidate. Voter can also view the election results after counting the votes done by admin.

System Architecture

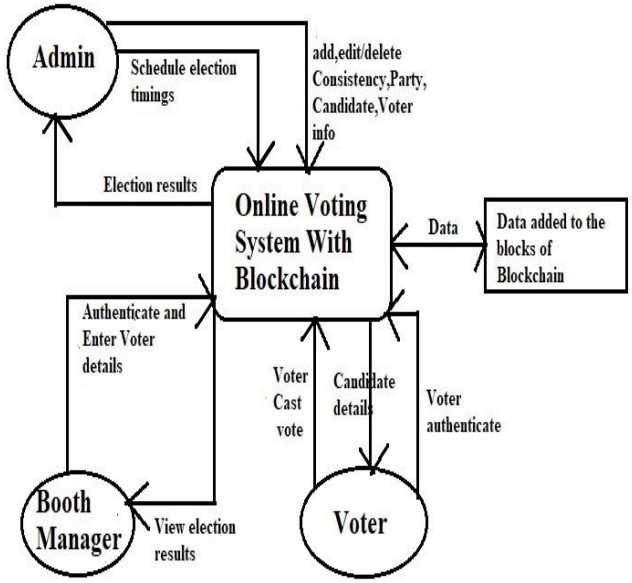

Figure 1 depicts how Admin/Election Officer, Booth manager/Incharger, Voter interact with Online voting system.

The Stages involved in the system.

a) Voter Authentication phase

The registration of voter details like name, gender, date of birth, Aadhar number, mobile number, mobile IMEI(International Mobile Equipment Identity) number ,address is done by the admin. Each voter record will be unique based on the unique Aadhar number given by voter.After the registration of voter ,the voter is provided with loginID and password .This loginID ,password is uniquely randomnly generated for each voter and should be kept secretly.

Firstly, the authentication of voter is done using Android based web login authentication mobile app , using a popular biometric security feature of smart phone i. e, fingerprint scanning and recognition technology. The voter will record his fingerprint, the Fingerprint recognition sensor is used to scan the fingerprint of the voter .

The voter opens the mobile app , his fingerprint is sensed and verified with already recorded fingerprint stored in mobile device ,If the fingerprint matches then the message "Account verified " is displayed in the app and the IMEI number of the mobile device is picked up and sent to the cloud storage . This IMEI number is compared against the IMEI number of the voter entered during registration in the cloud. If the match is found and vote status flag of that particular voter is set to 1, then that particular voter will be eligible to vote. If fingerprint doesnot match then the error message "verification failed" is displayed is in the app Secondly, the voter will login using his loginID and password provided during registration ,if loginID and password matches and vote status set to 1, then voter is directed to web page to cast his vote . .Suppose the voter doesnot have smart phone then IMEI number of that voter is entered as zero during registration and the voter has to go the booth of his respective constituency , the booth manager/Incharger will login using his loginID and password and then enters into portal where he enters the voter loginID and password , If the loginID and password of the voter entered matches then voter is directed to web page to cast his vote, otherwise an error message is displayed .

b) Voting phase

The voter after authentication will proceed to cast his vote. The voting time is scheduled by the admin, when voting starts the Candidate list, Candidate party, party logo belonging to the voter constituency is displayed on the web page , then the voter will choose the right candidate and cast his vote by clicking on the vote button, If the voter is not interested to vote any candidate then, he can cast Nota vote . After voting , the vote status of that particular voter is set to "Cast Vote" ,so that voters will get the chance once to cast his vote.

After Successfully Casting the vote, the database dynamic table with tablename of "Constituency ID _ Candidate ID" is created ,if table is already created then update the entries in the table. For each and every candidate belonging to each constituency the separate dynamic table is created. This dynamic table acts as a Blockchain. Each entries in the Blockchain refers to a single transaction blocks of Blockchain. Each block contains the information about the SerialNo, constituency ID, Party ID, Candidate ID, Voter ID, Previous Hash Value. The initial block in a Blockchain is known as the 'Genesis block' or 'Block 0'.First the genesis block is initialised and contains NULL value, then 'Block 1' is created and its Hash Value is stored in the genesis block , transaction cannot be modified because each block keeps a record of the previous block. The Block data is encrypted using SHA one-way hash function that cannot be reversed. Each blockdata is hashed using SHA256 algorithm and placed in the previous block Hash Value field. Likewise, every block is created and distributed among various servers, to provide the high fault tolerance. Everytime the voter cast vote , depending on the candidate he selects, the new block is added in the corresponding Blockchain. The Blockchain is created based on number of candidates standing .

In case if voter selects on Nota vote then a separate table is created with the tablename "constituencyID_nota " is created, and then further the table is updated with new blocks.

c) Counting phase

The votes casted for candidates is calculated by admin, and can be viewed by voter who casted vote. When the admin selects the constituency, party ,candidate from the drop down list and click on candidatecount button ,then using the constituency selected, the voters belonging to that particular constituency are obtained. Then generate the hash value of selected "constituencyID_partyID_candidateID_voterID" using SHA256 algorithm and compare the hash value with the corresponding "constituencyID_candidateID" table if the match is found ,then the count variable for the candidate is incremented and the new row is inserted in ElectionResult table, if the entry for candidate exists in the table then the count variable value of that particular candidate is updated.

Finally, the candidate with the highest count value is declared as winner of the election for that particular constituency. The admin will announce the winner of the election for each constituency .The election results is displayed on the web page along with Candidate Name, Candidate's party and the Count value .

Each Voter will login with his loginID and password , and can view the election results.

d) Vote Tampering and Recovery phase

In Tampering phase the voter who has casted vote will tamper the data. The voter belonging to particular constituency will tamper the vote data of candidate belonging to other constituency. The voter will retrieve the records of all the voters in the consistency ,and then by clicking on any voter from the list will tamper the candidate's vote count of other consistency. after tampering the Data if admin performs candidate count then the message "vote record Tampered " is displayed on the web page.

In Recovery phase , the admin clicks on the recover button, Since Blockchain is distributed ledger, then Blockchain data is stored on multiple servers or nodes hence the data is retrived from other server /node and recovery is made.

IV.RESULTS AND DISCUSSION

Blockchain based Online voting is not just one of the service rendered by Blockchain technology. For a fruitful Online-voting system requires several major important features to satisfy. Security and protection issues are one of the most basic components since we need to avoid from having the option to control the results by any parties and keep up the political decision honesty.

We acknowledged that Blockchain had improved a segment of the security and protection aspects. Yet, it ought to be still improvement. To ensure the counted votes are authentic .different properties should be remembered for e-voting systems based Blockchain are:

- **Accessibility:** This Voting System is open to all voters if the web association is accessible , with the goal that voter can make choice from his area, consequently urge everybody to cast a ballot. This system has no technical issues that makes casting a ballot impossible for certain sections of the population.
- **Transparency:** Transparency makes a reliable political decision election, solves the questions about altering and distorted outcomes. Hence transparency is achieved in Blockchain.
- **Security :** All that happens on the Blockchain is encoded and it's conceivable to demonstrate that information has not been modified, because it is decentralized. So it is excessively secure. In this system Tampering of votes is done and recover of the votes is made correctly and accurately.
- **Processing time :** Current voting systems often some effort to gather and compute votes. When voting stations are in various territories and workplaces are not all together, it very well may be hard to assemble all the data rapidly and proficiently which prompts time and cost issues. Instead of having to wait for a large number of people to communicate manually, all coordinators will have the option to see the result in a split second on the Blockchain. Results can be assembled and prepared rapidly after the voting has finished. This system provides results of count of votes within few nanoseconds.
- **Anonymity:** In e-voting systems, People need protection while casting a ballot and furthermore don't have any desire to unveil their votes It can prompt harassing or pressure if the government, opposition party, or anyone else can find out who a person voted for. This may help many people to participate in voting process and use the voting system. This anonymity of the voter still requires improvement.
- **Scalability:** The time the transaction put into the block remains in the block until it is truncated from block, and the time to reach the agreement still needs an improvement.

V. CONCLUSION AND FUTURE SCOPE

In this paper we develop an Online-voting system using Blockchain which is more convenient for the people having computer, or a mobile phone. This system will transform the way elections are the conducted in future. Also, the voter can participate in direct democracy and make the right administrative decision. This Online voting system using the biometric feature i. e, fingerprint will allow only the authenticated voter ,hence it avoids invalid candidates. This System exhibits high transparency in the voting process . This system is automatic and reliable as it manages to count the votes more securely immediately after voting is completed. Since Blockchain is a decentralized public ledger, the ballots results are more secure, cannot be modified by an individual. This Online voting System can be made the future for our voting

process and hope it could be implemented more effectively.

This project is limited for small-scale polls and elections such as college elections. In future work, For countries of greater size, the feasibility for large-scale election should be analyzed. A android mobile phone app of E-Voting system can be built.

REFERENCES

[1] C.Sravani, G Murali, "Secure Electronic Voting using BlockChain and Homomorphic Encryption",International Journal of Recent echnology and Engineering (IJRTE),**ISSN: 2277-3878**,Volume-**8,** Issue-**2S11**, September **2019**.

[2] V. Sahaya Sakila,Debin Jose, Abhijith K P, Adith R Babul,"Secure Online E-voting Protocol Based on Voters Authentication", International Journal of Innovative Technology and Exploring Engineering (IJITEE),ISSN: **2278-3075,** Volume-**9**, Issue-**1**, November **2019** .

[3] A. Singh and K. Chatterjee, "Secevs: Secure electronic voting system using blockchain technology," In the Proceedings of thedef 2018 International Conference on Computing, Power and Communication Technologies (GUCON). IEEE, 2018, pp. **863–867**.

[4] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "Evoting with blockchain: an e-voting protocol with decentralisation and voter privacy," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing(CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018, pp. **1561– 1567**.

[5] Jason, P. C., and Yuichi, K," E-voting system based on the bitcoin protocol and blind signatures", IPSJ Transactons on Mathematical Modeling and ts Applcations, Vol.**10** No.**1 14-22,Mar.2017**.

[6] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim,"Electronic Voting Service Using Block-Chain", JDFSL, Volume **11**,**2016**.

[7] Yifan Wu,"An E-voting System based on Blockchain and Ring Signature",Copyright c 2017 School of Computer Science, University of Birmingham,**2017**.

[8] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain." ,IACR Cryptology sssePrint Archive, vol**. 2017**, p. **1043, 2017**.

[9] J.-H. Hsiao, R. Tso, C.-M. Chen, and M.-E. Wu, "Decentralized e-voting systems based on the blockchain technology," in Advances in Computer Science and Ubiquitous Computing Springer, **2017**, pp. **305–309**.

[10] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," International Journal of Electronic Government Research (IJEGR), vol. **14**, no. **1**,pp**. 53–62, 2018**.

[11] Darshak N,Gautham A N, Veera Sandeep M , Gopal Krishna shyam," Blockchain Enabled E-Voting System", International Journal of Computer Sciences and Engineering (IJCSE), ISSN: **2347-2693** Vol.-**7**, Special Issue-**14**, **May 2019.**

[12] Yash G. Gupta,Arun kushwaha,Amar S. Rajeevan,Bhagyashree Dhakulkar," E-Voting using Block Chain Technology", International Journal of Computer Sciences and Engineering (IJCSE), ISSN: **2347-2693** Vol.-**7**, Issue-**5**, **May 2019.**

AUTHORS PROFILE

Dr.Prasanna B T is Currently Working as Associate professor in the Department of Computer Science and Engineering. He has both industry and teaching experience. Educational qualification includes B.E. (CS&E) from Siddaganga Institute of Technology,Tumkur, M. Tech (CS&E) from UBDTCE, Davangere and Ph.D (CS&E) from VTU, Belagavi. His research interest is in the areas of Computer Networks, Security, Cloud Computing, IoT, Machine Learning.

Mrs Rakshitha R pursed Bachelor of Engineering from JSS University, Mysuru in year 2017. She is currently pursuing Master of Technology from JSS University,Mysuru. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education.

