DESIGN A SMART E-VOTING MODEL: DECENTRALIZATION USING BLOCKCHAIN

Shantanu Bindewari[1], Prof. Jayesh Surana[2]
[1]*M.Tech Scholar (Information Security), Shri Vaishnav Vidhyapeeth Vishwavidyalaya, Indore (M.P)*
[2]*Assistant Professor, Information Technology, Shri Vaishnav Vidhyapeeth Vishwavidyalaya, Indore (M.P)*

Abstract: The main aim of this paper is to use a different cryptographic technique that would change the method of processing the election voting system especially using a secret ballot. Whenever a person tries to make his contribution to the economy of the country by voting it is the duty of the commission to provide the voter with the Assurance that the vote they have cast has been properly recorded and cast into the system. It is the duty of the election commission to conduct a proper election without any form of violation of codes including the process of altering the minds of the people. The commission should take proper steps to ensure that even the people who are willing to change their mindset can allow themselves to be influenced by others should not change. Even though the current Technology has been using multiple forms of voting including online voting it's finally required certain humans to do the final calculations and announce the result. The present method of using normal voting system is not suitable as they do not provide the essential assurance. So in order to ensure that the voter's vote properly using block chain entered and to check the credibility various techniques like homographic encryption and ring signature and pork are measured. The main aim of this paper is to measure the credibility of the current system.

I. INTRODUCTION

Most of the countries consider the election as an important part of their democracy and problems in the election is considered as a major threat and shame to the country. So continuous researches are made to create a proper voting system. The aim of this research is to increase the system of voting in a more secure and less costly way. Right from the start people have always been using the system of pen and paper to cast their votes but right now the recent research to replace this method with an efficient method that will provide more security is becoming more and more essential. People use

Normally two methods of voting like the electronic method of the normal traditional pen and paper method. But both these metals have their own defectives which are low the third person to easily Alter The Woods and change the minds of this person through various coercion methods. The aim of this paper is to increase the security and integrity of the elections by using various methods.

1. **Consensus Protocol:** when using a blockchain method the main technology that is being used is is a nodal technology. In thosethods, all the nodes available in the system is given the entire information rather than giving single information of that area. So even if one node is destroyed then the other nearby possible nodes can be used and retrieved. In this method, the power is distributed equally across all the nodes and hence they lack a central system which prevents it from getting destroyed. So even when the attackers decide to attack a single node the data can be easily retrieved from the other node available. So changing the information in a particular node will not change the final result of the election and the attack on a particular node can be easily identified. All the nodes are protected by block information and order to enter a particular node the person needs permission from all the block information which might be difficult to obtain in case of certain illegal transactions.
2. **Cryptographic:** Each and every single block available is being connected to each other with the help of a timestamp. For example, the previous and the upcoming block are being connected to each other with the help of a SHA256 hash algorithm that protects all the block through the connectivity and safeguards the integrity E from various attackers.

Security and Coercion-Resistance Analysis

With the help of certain assumptions the Tosecuroty and coercion resistance can be easily verified. Some of the common assumptions that are being used are the first assumption is that the voters are casting their vote in a secure my life without any disturbance or intrusions. The next assumption is that usage of the nodal system to ensure the the security of the complete system and prevent them against attackers. The entire election process should be recorded with the help of the digital medium on various video devices in such a way that it would not invade the privacy of the voter.

Technically it would be highly impossible for a person to attack the system of nodes especially with the help of a blockchain system and use various social engineering techniques to change the the voting results. But even then proper security should be made to protect the secret key and other encryption details of the voting system. It is essential that irrigate should cast their vote without the assistance of any person standing near or behind them. The researchers have detected that at the only way the voting system can be Attacks is by two different methods.

a) Man-in-the-Middle Attacks

This method can be easily avoided because once the voter enters the personal detail along with their vote the system immediately encrypts the data and send them to the node. It would be highly impossible for a person to you alter an encrypted data especially without knowing the security key. Also the public key that is being used for protecting the the systems are entered within the blockchain system making it difficult for a person an to attack the blockchain and the original key with a duplicate one due to the presence of multiple number of nodes. This also protects the leakage of the ballots.

b) Denial-of-Service (DoS) Attacks

DoS attack is a severe problem for the servers that are centralised. The method of using the nodes is a good concept since they are extremely decentralized and hacking one particular node will not destroy the information available. All the data are been stored in every single node and hence attacking on destroying on particular node will not do any change in the system.

With the help of the blockchain technology a proper biometric system is used for identification and voting.

The current voting method is being completely changed in such a way that when there is any change that has been made in the system between the voting system and the telling period can be easily detected Technology. in this method with the help of a proper blockchain Technology we use a method to to remove the usage of the bulletin board and provide more privacy to the voter. The system will work in a perfect way even when there is a single node that is working perfectly. In this paper section II clearly describes the major problems available in the voting system and explain the blockchain technology and how they prevent the voters information from attack. Section 6 provides detailed on how voter is identified and how their eligibility is decided. Section III provides information on the process of voting on the records that have been take and and how they are used for counting and Security features of our voting system. they keep them private and finally section IV provides the final remarks on the conclusion.

II. RELATED WORK

Continuous researches have been done in the past 20 years with multiple number of techniques for voting system especially in case of exciting. Multiply number of techniques have been continuously introduced by the researches and among the various techniques introduced there were only few techniques that were useful. The are Votegrity [1] (proposed 2 by Chaum), Markpledge [3], Pretˆ a Voter [4], STAR-Vote [5], Blockchain validation nodes. Depending upon the common belief that it administrator will not disclose the personal security key the blockchain technology is being used with multiple number of nodes where each and every single node contains all the information so that destruction of one node will not destroy the complete process. this paper provides a detailed explanation about the liquid technology and usage of zero Concept for or encryption technique to prevent the duplicate use of signature And replacements. The whole section in detail explains the the process of election system that includes,

(1) identifying and authenticating the ballots (check whether the ballots are from the same voters and/or check whether the given ballot encrypts only one candidate),
(2) Check the validity of the signature on the given ballot,
(3) ballots tallying, and
(4) verify the correctness of the voting result.

Also in this technology the voters have to pass through certain qualifications through the blockchain interface in order to to input their vote. If they cannot then the year what is cancelled and regarded as invalid. All the political parties and the contestants can be given a separate node for a proper trustworthiness and also to prevent the process of false voting.

III. PROPOSED METHODOLOGY

Security features of our voting system –

In this method a proper Merkle hash tree technology is being used to store the required data. There are two types of blockchains the private and the public. The private blockchain are being used for saving the data since they are much different from the other forms of blockchains and the public blockchain is used to store the encrypted data. In the private blockchain authenticated and analyze the person can enter and delete the registered information at the end of the election process to make sure that they cannot be misused. A proper person with the proper knowledge can perform this activity including data mining. During the registration process the process of Administration is owned by the administrator but during the voting process the administration process is owned by the machine. Also the voters list should be displayed to everyone so that anyone who cannot access them can inform and prepare a duplicate one the complete voters list information should be updated at least two weeks before the election. The administrator should update continuously about the the data.

To maintain the privacy of the what does each and every single ballot available in the registration are being encrypted and other than the administrator no other person should have the ability to decode the ballot data. As a result only the administrator has the ability to open the data in the final accounting centre.

The Identity of the voters under the candidates should be completely protected within the public key and no one other than the the official administrator should know about them. With the help of the linkable Ring signature skin identity of the voter can be easily protected. Also in the system there are multiple number of double voting available which is not

possible with our voting system since the system will automatically generate the duplicate signatures and alert the

a) Administrator : As a result the voter can provide a signature only once and register their ballot also only once. The system has the ability to detect the duplicate signatures and similar signatures also with the help of the LRS scheme they provide a proper guarantee for this safe voting.

b) Slander ability-avoided: it is impossible for a voter to create a duplicate signature that are interlinked with other forms of Signature which are not generated by them. For example it would be difficult for a person to create a duplicate signature especially while using the bio metric system.

c) Receipt-freeness: also even if a person after various passivation attains the personal key of the water then and in attached to that an additional ciphertext of zero is being added to the encryption to prevent these types of duplicate votes and they are unknown to the voter. So without proper analysis and dot integration it would be difficult for a duplicate voter enter and perform changes in the database. So even with the help of the secret key it might be difficult for the water without the proper ciphertext encryption available. Along with the zero Technology flip coin technology is also being used where the validity is being authenticated by the nodes instead of zero a random number is being added before the data to provide proper encryption.

d) Public verifiability: any person with the proper verification system can use the technology of blockchain and check the process of voting and if the voting system is been happening properly and whether their votes are being recorded.

e) Correctness: This method clearly indicates exactly how correct the voting process is and how detailed the participation is being recorded without any form of slandering. Every single person who has voted should provide proper proof and their interactions with the blockchain system. Even if an particular node is destroyed with the help of the multiple other nose verification process can be easily completed without any problem.

f) Vote-and-Go: there are various types of voting systems available and when compared to the previous voting system that is not a requirement from the voter to initiate the process of counting. Hens anyone who wants to cast their vote can attend and finish their vote casting and leave the premises even before counting process begins.

In the new solution the blockchain technology uses only one type of transaction and with the help of other types of systems and has system the chains are interlinked from one has to another providing a proper systematic type of voting

Comparison with other non-blockchain-based voting protocols Compared with other non-blockchain-based evoting protocols:

The voting system followed by our country is of three major types and they depend upon three types of security system. Initially the centralization of the voting system should be avoided and the process of tallying and integrity should not be restricted to one party. In this method of using block chain Technology the system is completely decentralized and hence it is impossible to hack and change the database. The usage of biometric system provides proper validation technique and replacing the person is completely impossible. Also during the process and while the final Tally all types of nodes are being used and the destroyed nodes can be easily replaced with the instructions from the other nodes. Also each and every single voter should free completely confident about the process and they can cross verify there validity in this method of blockchain process.

There are two types of checking system that check the authentication of the voter. Initially when the voter presents themselves with the receipt the checking is done and ballot is been confirmed point also secondly all the reports collected should be cross checked with the system. Type of verification reduces the the interaction of the extra person in the middle and they also prevents the the ballot from getting attached. Send to hack the database they should go through with three initial steps and they are also need certain private keys and the availability of multiple number of nodes prevents the attacker from attacking since they have to delete the entire database and redo them again. They require a lot of time and money which is not possible.

IV. CONCLUSION

This paper clearly provides various methods that can be used to who conduct the elections in a safe and Secure way and also so we protect the the information of the voters by using our blockchain technique encryption method. The system that is being applied nowadays is the usage of hash algorithms that protects the privacy of the particular person then and allows them to vote freely without any intention. The final casyed notes are also protected effectively through the usage of a nodal system. Hence with the help of bloackchain methods with a proper nodal system the information is stored securely in all the nodes.

V. REFERENCE

[1]. Francesco Fusco1, Maria Ilaria Lunesu2, Filippo Eros Pani2 and Andrea Pinna2," Crypto-voting,a Blockchain base de-VotingSystem"KMIS_2018_41_CR.

[2]. Abhishek Kumar1,Ashok Kumar Srivastava(2011) ,"Designing and developing secure protocol for mobile voting"International Journal Of Applied Engineering Research, Dindigul Volume 2, No 2, 2011

[3]. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson," Blockchain-Based E-Voting System"E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy,arXiv:1805.10258v2 [cs.CR] 3 Jul 2018

[4]. Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today.
[5]. TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain/
[6]. Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/ [5] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper.
[7]. Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/ 13183222.2015.1017264#.Wr0zCnVl8YR.
[8]. Ernest, A. K. (2014). The key to unlocking the black box: Why the world needs a transparent voting dac.
[9]. McCorry, P., Shahandashti, S. F., and Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. IACR Cryptology ePrint Archive, 2017:110