Secure Digital Voting System Based on Blockchain Technology - A Survey

Kantharaju. V[1], Dhanalakshmi M. V[2], Nidhi[2], Deepa B[2], Almas A[2]

[1]Assistant Professor & HOD of ISE Department, KNS Institute of Technology, Bangalore, Karnataka, India

[2]Student, KNS Institute of Technology, Bangalore, Karnataka, India

ABSTRACT

Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations - voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large - scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain- based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed. Due to these concerns, it was determined that the existing frameworks need to be improved to be utilized in voting system.

Keywords : Blockchain Technology, Electronic Voting Systems

I. INTRODUCTION

The phenomenon of highly respected representatives' opinions is in form of electoral institutions. These electoral institutions vary from university unions to parliaments. Over years, "voting" has become a tool used to express people's willingness to choose among existing choices. Voting tools help increase people's trust in the choices made with a majority of votes. This will help to balance process and increase value of electoral system. As people's faith is increasing in democratic countries it is necessary not to let people lose trust in voting and voting system. Relying on the growing trust in democratic system, voting process has become a plan that can help people elect representatives and thus form a government. Representative office reassures the people and convinces government that government should pay attention to national issues, such as national security, health and education policies, etc., for benefit of people. To make voting process more effective, institutions such as election committees have been established in different parliamentary democratic systems. Many procedures have been introduced to conduct free, fair

and transparent elections. Confidential voting also introduced in beginning of voting system. Trust in democratic electronic voting is increasing, and maintaining this trust is important. Earlier voting process was not hygienic and had many problems.

II. LITERATURE SURVEY

1] Authors: V. Sahaya Sakila, Debin Jose, Abhijith K P, Adith R Babu.

Main objective of Secure Online Electronic Voting Protocol is to make sure the fair voting for users. Voting process is encrypted before the voter's electronic vote is submitted to server. Finally, the final result is classified by decrypting received encrypted information. Compared with other electronic voting systems, the advantages of this system are more effective because without extra cost and effort voters can vote from their devices, and for security encryption is used. Disadvantage of this system is that unfair voting can be conducted by expired voters.

2] Author: Ronald L. Rivest.

In Threeballot voting system, each voter casts three paper ballots with restrictions on how they may filled out, so the tallying works. These paper ballots are voter-verifiable. Advantage of ThreeBallot is to provide a nice level for end to end verifiability the voter gets guarantee that her vote was cast as intended and counted as cast, and that election officials have not interfered with collection of counted ballots. Disadvantage of this system is that ThreeBallot's power to vote buying is not strong.

3] Author: David Basin

Electoral security and economic election security system is an important social issue, because attacks on elections put democracy at risk. It is determined that election system is safe, it is necessary to reason about environment in which system is used. In security community, someone provides an adversary model that specifies some functions and assumes that it will use these functions independently of cost. For election security, system is usually designed to assume that there are quite powerful opponents that may damage customer platform but not voting server or postal channel. Election hacking is a major problem for democracy and an important research direction for both information security and economic research.

4] Authors: Nir Kshetri and Voas

E-voting is among the key public sectors that can be confused by blockchain technology. The ides in blockchain enabled E voting is simple. To use a digital currency analogy, and other issues each voter will have user credential. Each voter gets a single coin representing one opportunity to vote. Casting a vote transfers the voter's coin to candidate's wallet.

The advantages of electronic voting: it can increase the speed of voting, eliminate ambiguity, and can improve transparency and clarity of voters. Disadvantages of electronic voting: The main challenge of deploying blockchain is immature technology.

5] Authors: Basit Shahzad and Jon Crowcroft.

The Veracious Electronic Voting discusses the effectiveness of polling process, hashing algorithms utility, block creation and sealing, data accumulation, and result declaration by using adjustable blockchain method. It claims to catch security and data management challenges in blockchain and provides an improved manifestation of electronic voting process.

III. SYSTEM ARCHITECTURE

a) Existing System

In Swiss Canton of Valais in March 2017, voters did not receive postal ballots. When re- issuing ballots, make sure that the votes of affected voters have been cast. System also needs higher safety, privacy and transparency to become reliable voting system. Rivest proposed the concept of providing voters with three votes, and after marking voters will cast all votes. Each vote has identifier, but the voter remains unknown when decrypting key. When making a table, associate the number of votes and select the options found in two votes, while rejecting the choice of one vote. If there are only two contestants or multiple contestants,

the plan may not be used effectively. Another disadvantage of this scheme is that if the votes are not inserted into the corresponding boxes correctly, the method is slow and human errors increase.

Vote proposes a business solution that handles token-based systems built on blockchain technology to make sure the mystery and safety of voting method. This result is more suitable for i-voting without using physical and biometric authentication of voters. However, token based system limits applicability of voting platform and cannot be effectively used in wide and complete election. The function of solution seems to have been weakened to meet the challenge. Blockchain developed for electronic voting can public or private.

However, in public blockchain, transaction content is still visible for everyone on blockchain. Therefore, it is necessary to encrypt content of block by using security algorithms, to keep content of block unreadable and. This makes transaction slower and power of electronic voting and blockchain is compromised. To solve these issues, it is recommended to use private blockchain. However, it should note that software development of blockchain-based electronic voting solutions may encounter many challenges, while mobile based solutions have their safety and privacy challenges, and need to consider some issues, trends and challenges. Develop social media applications for such systems.

The country's Election Commission organization maintains private or consortium blockchain. This has its problems and requires solutions. In a private blockchain, only qualified nodes can see detailed information about voting and transactions, while voting process is still invisible to voters. Compared with paper-based voting, this makes voting process less transparent.

IV. Proposed System

Application of blockchain in reliable E voting is determined that the existing blockchain may require to be adjusted for following reasons.

- Block Creation: Creating a block during election process is a basic entity. If block is not created, voters will not be able to record their votes. It is therefore crucial to create blocks to form proof of work without solving mathematical problems. Since its consortium blockchain, proof of stake is irrelevant and burning coins not applicable, because mined block will be there with single person.
- Block sealing: Voters votes and transactions recorded in blocks. By end of voting, these blocks needed for hash function and use of Merkle trees and nonce functions. The concept of sealing does not exist in this process.
- Polling Time: As voting process will last from eight to ten hours, it is critical to create, seal and to fix block during this process. Since proof of work, proof of equity and burn proof can only be applied after a very long process, they are not suitable for use in trusted electronic voting.
- Result Delay: When polling process is completed and result has come, there is no need to continue block creation process. Since both proof algorithms will continue to repeated recursively, lot of computing power will use many times. This system does not use too many resources, thus maintaining cost, time and efficiency.

V. SYSTEM METHODOLOGY

- Entire modeling of electronic voting process.
  This method helps to draw whole system on paper to understand it clearly and rectify errors and processes that can observed before implementation.
- Identify appropriate technology platform to make sure the study, privacy and security:

Electronic voting process requires functions such as privacy, security, and variability as core functions of this solution, so choosing basic technology in order to overcome these challenges is important. It has determined that blockchain is sufficient to meet all these challenges.

Development and technology integration using perceptual electronic voting models

According to system model, it will be developed and integrated with standard technology.
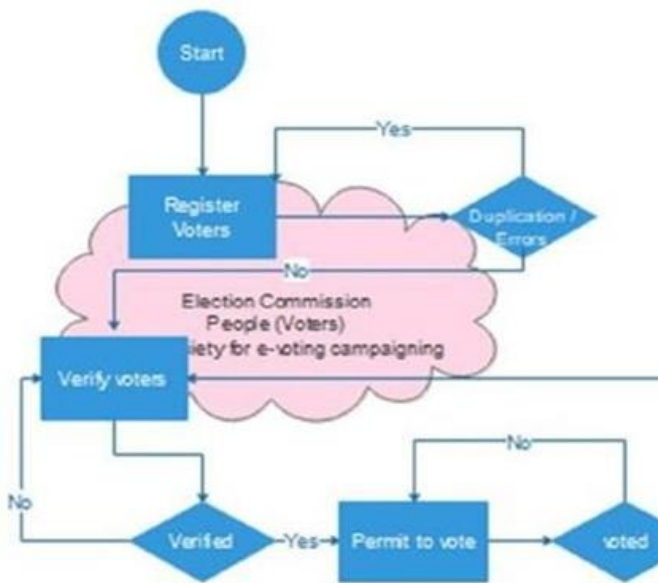

Figure 1 : Electronic voting process involving institutions.

Implementation of electronic voting system places huge individuals at different levels. It is necessary to understand the actual implementation for developing effective block creation system. In the election process, election committee and NADRA can play an important role. NADRA is a Pakistani registration agency responsible for registering and issuing documents to Pakistani citizens.

Responsibility of NADRA is to make sure that each citizen of country has its available records, and provides biometric information for everyone. On the polling day, biometric authentication is used to authenticate voters. The Election Committee is responsible for providing a list of elections that can be verified from basic records.

Voters who have authenticated can vote according to regulations which given them, and use technology to record votes and list the tables respectively. When polling station and constituency tabulation are completed, election committee also has responsibility to announce the results. Figure 4 indicates flow of activities and corresponding institutions and related technologies.Pakistan is chosen as example in this project; the national assembly held 272 direct national elections. For voting, constituency is divided into polling stations. According to number of voters in area polling stations may vary.

Each polling station managed by host, and the host is given assistants and some personnel. Responsibilities assigned to each staff member are to identify voters and help him vote without fear and influence. This is solution based on biometric authentication of electronic voting machines and voters before voting.

Voting includes following steps.

- Name of voter must be on voting list so that he can visit polling station to vote. Voters themselves are responsible for ensuring that their names should appear on voting list once they reach the age of eighteen. This can be done by consulting the respective office, such as National Database and Registration Authority. Voting list was announced several weeks before election. Individuals with names on voting list are eligible to vote that show voters identity. Voters must be authenticated through biometric system before voting. Check voter records with the help of database.
- Once the voter passes identity verification check he is taken to voting screen. From voting machine, names of each candidate and their respective party symbols are displayed, voters can vote according to their wishes. The confirmation screen needs verification from voters and records vote.
- Voters can only vote once. After voting the record will be marked as 'voted', which restricts voter to vote again. Once voted, names of voters will

removed from list of current election. In his online voting work, he proposed a framework that allows voters to vote multiple times, and each vote will cancel previous one.

· The voting process continues until all voters in voting list have voted.

· Display polling station results and list of votes obtained by candidates. This process will repeat for all polling stations and mass results will constitute result of that particular constituency. Similarly, results of all constituencies are collected to add up results of national election.

VI. CONCLUSION

Even in developed countries, distrust of voting is not uncommon. However, electronic voting has become an option, but it has not yet been implemented on large scale. E-voting is expected to have bright future. In some countries, electronic voting is not possible, and few people are eliminating security, verifiability, and anonymity issues. The proposed framework is based on blockchain technology that can understand the problems in polling process. Choose appropriate hash algorithm and adjustments in blockchain, voting data management process, security and identity verification of system. The function of blockchain has been adjusted and used to adapt dynamic changes in this system.

VII. REFERENCES

[1]. R. Silhavy, P. Silhavy, and Z. Prokopová, 'Architecture of COOPTO remote voting solution' in Advanced Techniques in Computing Science and Software Engineering. Dordrecht, the Netherlands: Springer, 2010, pp. 477-479.

[2]. D. Basin, H. Gersbach. A. Mamageishvili, L. Schmid, and O. Tejada, 'Election security and Economics' it's all about eve, in Proc. Int. Joint Conf. Election. Voting, 2017, pp. 1-28.

[3]. N. Kshetri and j. Voas, 'Blockchain- enabled e-voting,' IEEE Softw., vol. 35, no. 4, pp. 95-99, Jul. /Aug. 2018.

[4]. F.P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson. 'Blockchain- based e-voting system,' in Proc. IEEE 11th Int. Conf. Cloud Comput. San Francisco, CA, USA, Jul. 2018, pp. 983-986.

[5]. A.B. Shahzad and A. Said, 'Application of quantitative research methods in identifying software project factors,' Int. J. Inf. Technol. Elect. Eng., Vol. 1, no. 1, pp. 30_33, 2012.

[6]. K. Saleem, A. Derhab, J. Al- Muhtadi, and B. Shahzad, 'Humanoriented design of secure machine-to-machine communication system for e-healthcare society,' Comput. Hum. Behav., vol. 51, pp. 977-985, Oct. 2105.

[7]. SpringerLink. Security Analysis of SHA-256 and Sisters. Accessed: Aug. 2, 2018.

[8]. R. L. Rivest, 'The three ballot voting system,' Tech. Rep., 2006, p. 15.